ACQUISITION RESEARCH PROGRAM
SPONSORED REPORT SERIES

Identifying Governance Best Practices in Systems-of-Systems Acquisition

8 February 2014

Project Directors: David Berteau and Guy Ben-Ari

Author: Joshua Archer

Center for Strategic and International Studies

Report Documentation Page		*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **08 FEB 2014**	2. REPORT TYPE	3. DATES COVERED **00-00-2014 to 00-00-2014**
4. TITLE AND SUBTITLE **Identifying Governance Best Practices in Systems-of-Systems Acquisition**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Center for Strategic and International Studies,National Security Program on Industry and Resources,1616 Rhode Island Ave, NW,Washington,DC,20036**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Acquisition governance currently confronts two problems: the growing size and complexity of systems-of-systems capabilities and the limited effectiveness of existing governance models to ensure the on-cost and on-schedule delivery of those capabilities. The Center for Strategic and International Studies (CSIS) is engaging in research on systems-of-systems acquisition governance best practices that could help the defense acquisition community overcome some of these problems. This report provides the results of several case studies illustrating the challenges of complex systems-of-systems acquisitions. It characterizes how existing acquisition governance models fall short of meeting the challenges of complex systems-ofsystems acquisition, and offers five best-practice themes meant to address those challenges based on the results of CSIS research and interviews with stakeholders in the acquisition community. Finally, it concludes that the attributes most critical to success in complex acquisition efforts are level of organizational focus, decisionmaking authority, and enforcement.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**81**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Abstract

Acquisition governance currently confronts two problems: the growing size and complexity of systems-of-systems capabilities and the limited effectiveness of existing governance models to ensure the on-cost and on-schedule delivery of those capabilities. The Center for Strategic and International Studies (CSIS) is engaging in research on systems-of-systems acquisition governance best practices that could help the defense acquisition community overcome some of these problems. This report provides the results of several case studies illustrating the challenges of complex systems-of-systems acquisitions. It characterizes how existing acquisition governance models fall short of meeting the challenges of complex systems-of-systems acquisition, and offers five best-practice themes meant to address those challenges based on the results of CSIS research and interviews with stakeholders in the acquisition community. Finally, it concludes that the attributes most critical to success in complex acquisition efforts are level of organizational focus, decision-making authority, and enforcement.

Keywords: System-of-Systems, Complexity, Interoperability, Program Management,, Governance, Acquisition Workforce, Defense Technology

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

THIS PAGE INTENTIONALLY LEFT BLANK

About the Authors

David J. Berteau is senior vice president and director of the CSIS National Security Program on Industry and Resources, covering national security plans, policies, programs, budgets, and resources; defense management, contracting, logistics, and acquisition; and national security economics and industrial base issues. Mr. Berteau is also an adjunct professor at Georgetown University and at the Lyndon B. Johnson School of Public Affairs, a director of the Procurement Round Table, and a fellow of both the National Academy of Public Administration and the Robert S. Strauss Center at the University of Texas. Before he joined CSIS full time in 2008, he was director of national defense and homeland security for Clark & Weinstock, director of Syracuse University's National Security Studies Program, and senior vice president at Science Applications International Corporation (SAIC), as well as a non-resident Senior Associate at CSIS. He served at senior levels in the U.S. Defense Department under four defense secretaries, including four years as principal deputy assistant secretary of defense for production and logistics. Mr. Berteau graduated with a B.A. from Tulane University in 1971 and received his master's degree in 1981 from the LBJ School of Public Affairs at the University of Texas.

David Berteau
National Security Program on Industry and Resources
Center for Strategic and International Studies
1616 Rhode Island Ave, NW
Washington DC, 20036
Tel: (202) 775-3136
Email: dberteau@csis.org

Guy Ben-Ari was a senior fellow and deputy director of the Defense-Industrial Initiatives Group at CSIS, where he worked on projects related to U.S. and European technology and industrial bases supporting defense. Prior to joining CSIS, Mr. Ben-Ari was a research associate at George Washington University's Center for International Science and Technology Policy, where he worked on European research and development policies and European network-centric capabilities. From 2000 to 2002, he conducted collaborative research and development programs for Gilat Satellite Networks Ltd., an Israeli high-technology company in the field of satellite communications, and from 1995 to 2000, he was a technology analyst for the Israeli government.

Joshua Archer is a research associate with the National Security Program on Industry and Resources at CSIS, where his research interests include defense economics, federal agency management, and international joint development

programs, particularly between the United States and Japan. Before joining CSIS, Mr. Archer worked for firms in the defense and aerospace industry as a strategy consultant between 2010 and 2013. In 2009, he was a researcher with the James Martin Center for Nonproliferation Studies, where he performed web development work and contributed to the Taiwan military capabilities profile of the Nuclear Threat Initiative database. He holds an MA in international policy studies from the Monterey Institute of International Studies.

Joshua Archer
National Security Program on Industry and Resources
Center for Strategic and International Studies
1616 Rhode Island Ave, NW
Washington DC, 20036
Tel: (202) 775-3106
Email: jarcher@csis.org

ACQUISITION RESEARCH PROGRAM SPONSORED REPORT SERIES

Identifying Governance Best Practices in Systems-of-Systems Acquisition

8 February 2014

Project Directors: David Berteau and Guy Ben-Ari

Author: Joshua Archer

Center for Strategic and International Studies

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

Over the last decade, researchers at The Center for Strategic and International Studies (CSIS) have observed the increased challenges of complexity in defense acquisitions. Through workshops, conferences, and publications, CSIS has examined how the government purchases complex systems, what challenges it encounters when it tries, and what key attributes of governance can be modulated to provide more effective acquisition.

Building on the work CSIS and other scholars have put into understanding complexity, this study asks one simple question: What best practices contribute to better, more efficient acquisitions? To answer this question, the CSIS project team revisited its past work on complexity in acquisitions, analyzed new scholarship on the subject, and conducted detailed interviews with executives from across the defense acquisition community. The result of this 12-month effort is a new model of acquisition governance.

In order to assess a model for complex acquisition governance, CSIS researchers began with the following assumptions about complex system-of-systems acquisitions. Although these are testable assumptions, such assessments are beyond the scope of this study. The first assumption is that formally embracing complexity in acquisition efforts is necessary. This assumption allows the research to avoid the tautology that the best way to manage complexity is to avoid complexity. Complexity emerges naturally in all systems, and the focus of this paper is how defense acquisitions can more effectively operate within it.

A second important assumption is that complex acquisitions share similar challenges that can be addressed with similar solutions. The challenges of complexity in one effort may appear different from those of another effort, but at its core the challenge of complexity is related to the unpredictability of interactions between systems.

The third and final assumption is that the agency or service that is acquiring a defense system-of-systems—the Department of Defense, a defense service component, or some other federal agency—is also the lead developer of that system. As the research demonstrates, warfighters have turned to developing or adapting their own solutions to threats they encounter in-theater. Given this trend, one solution to acquisition challenges might be to allow end-users to innovate more systems. However, the focus of this paper is specifically on those systems that require the time and resources that only a large enough organization such as the Department of Defense is capable of building.

This report outlines best practices based on eight CSIS-developed governance attributes. The report concludes that three attributes in particular are indispensable to getting governance right. One is that acquisition leaders must ensure that their organizational focus is at the right level, with sufficient fluidity. The second is that they must delegate authority so that capabilities-level program managers have sufficient autonomy to select and develop sub-systems, while maintaining the authority to direct them toward enterprise-level objectives and standards. Lastly, executives should put into place enforcement mechanisms tailored to the specific challenges of their acquisition efforts. The report describes in detail associated best practices that support these three critical attributes, as well as the five remaining enabling attributes.

Identifying Governance Best Practices in Systems-of-Systems Acquisition

Introduction

In this age of diverse and evolving security threats, the defense community is acquiring weapons, platforms, and systems with greater complexity. Here, the term *complexity* is used to describe systems-of-systems (SoS) involving multiple, interrelated elements that interact unpredictably. As defense products and capabilities become more complex, they are stressing the structure necessary for the acquisition of defense systems-of-systems. As a result, the acquisition community has encountered operational challenges in maintaining a sufficient engineering and acquisition workforce and process, as well as cost and schedule challenges.

SoS acquisition poses considerable challenges that the current Department of Defense (DoD) acquisition governance structure was not necessarily designed to address. Increasingly, defense capabilities must support the needs of multiple users and must operate as horizontally integrated systems incorporating multiple individual platforms and programs. The high degree of interoperability and collaboration required for these SoS capabilities necessitates not only advanced systems engineering capabilities, but also advanced governance. Because the technical capabilities needed to achieve national defense missions have grown beyond the existing models of governance used to acquire them, the DoD faces challenges in developing, procuring, and deploying next-generation weapons and platforms. Furthermore, cost growth in its portfolio of accounts demonstrates that the DoD is encountering challenges managing cost and schedule risks associated with advanced and integrated capabilities.

Attention to governance is often lacking, and the literature on this aspect remains relatively scarce. The acquisition community tends to address the challenges of complexity from a technological standpoint, with recommendations for improvements focusing on issues such as better knowledge management tools, modeling software, and systems engineering. Less common, however, is the kind of effective governance critical to the successful delivery of complex SoS capabilities. Governance ensures not only accountability and oversight over delivery, but determines proper resource allocation and risk assessment and management.

The application of good governance is essential to easing complexity's adverse impact on the outcomes of major acquisition efforts. As the acquisition community moves toward greater complexity in its major programs, schedule delays

and cost-overruns plague many of its Major Defense Acquisition Programs (MDAPs). This is partially attributable to risks associated with the highly interdependent nature of systems-of-systems and the DoD's heavy dependence on developmental technologies within complex acquisition efforts. These two factors in particular contribute to malfunctions and failures at the sub-systems and components levels. Good governance facilitates effective risk management to lessen the impact of complexity on program outcomes.

Good governance also helps mitigate process burdens associated with the DoD's larger acquisition undertakings. The lack of a centralized management authority in a complex acquisition effort can create confusion among stakeholder agencies and contractors. It can also widen the gap between enterprise-level and sub-component objectives, creating a greater potential for resource misapplication and decreased tactical value to the warfighter. Finally, it can hinder effective allocation of human capital for technical and program management functions. These process inefficiencies can and often do impede the ability of the government to realize the benefits of a complex approach to acquisition.

Given the importance of good governance within complex acquisition efforts, it is critical for acquisition leadership to understand and operationalize what good governance is. The research presented here uses the previously established CSIS framework of eight governance attributes to identify best practices correlated with the successful acquisition and delivery of systems-of-systems.

The research analyzes two models for the acquisition of national security systems-of-systems: (1) the current model, in which programs-of-record (PoR) are acquired by an individual entity; and (2) a posited model of enterprise-wide coordination across multiple programs, platforms, or systems. CSIS began from the premise that the traditional, service-centric approach to acquisition governance may not be best suited to meeting the demands of managing complex acquisition efforts.

This paper presents a case study analysis of seven acquisition efforts representing both the traditional and enterprise-wide governance models (see Table 1). In addition to the large body of literature available on each of the cases, the research also uses in-depth interviews with program executives and thought-leaders in the acquisition community to extract eight descriptive governance attributes for each of the seven separate case studies. It summarizes those attributes most strongly correlated with more efficient processes and more effective outcomes in order to develop a best-fit model for complex acquisition governance, and a set of best practices for dealing with complexity in defense acquisition efforts.

Table 1.   The Center for Strategic and International Studies SoS Governance Case-Study Programs

Traditional Governance	Enterprise-Wide Governance
• Future Combat System (FCS) • Integrated Deepwater System (Deepwater)	• Counter Rocket, Artillery, and Mortar (C-RAM) • Distributed Common Ground System (DCGS) • Global Nuclear Detection System (GNDS) • Harvest Hawk • Maritime Domain Awareness (MDA)

Structure and Methodology

This report is divided into four sections. The first section defines complexity and its historical roots in defense acquisition and explores problems associated with complex SoS acquisition efforts. The second section presents seven case studies for both the traditional approach to acquisition governance and its enterprise-wide variant. Specifically, it details the seven SoS case studies outlined in Table 1 and conducts cross-analysis of the selected case studies using the results of CSIS interviews with program executives.

The third section presents the results of the analysis in the previous sections in order to construct a new model for SoS acquisition governance. It summarizes governance best practices using supporting evidence from specific case studies.

In order to summarize and present a new model for SoS acquisition based on governance best practices, CSIS conducted this research effort in three phases:

> **Phase 1**: Data collection and processing of SoS governance best practices
>
> **Phase 2**: Data validation and analysis of findings
>
> **Phase 3**: Conclusions and visualization of key findings

Phase 1 of this study focused on the collection of data and the processing of initial findings regarding best practices in SoS governance. CSIS gathered foundational information for this phase through a high-level review of publicly available literature on each of the programs and related themes, such as organizational behavior and program management theory. Researchers then conducted semi-structured in-person interviews with SoS program executives and systems engineers from the seven case study efforts. Other interviewees included SoS acquisition experts from the government and industry acquisition community not otherwise directly affiliated with any of the seven case studies. In the absence of governance data in the existing literature, these interviews served as a tool to

provide data for original qualitative analysis of SoS acquisition. CSIS finalized its initial analysis by applying its eight-attribute governance framework to the findings obtained during this phase. That framework is presented below:

- Level of organizational focus: The level at which SoS governance occurs within the organization. This is not the same as systems/capabilities focus or technical focus, both of which are outside the scope of the CSIS SoS governance analysis.

- Integration of functional end-user needs: The mechanisms and frequency with which the functional needs of end-users are built into the SoS, and at which points in the process of delivering the SoS this incorporation occurs.

- Decision-making authority: The governance mechanisms for SoS delivery, including how budget is allocated, standards are set, tradeoffs are managed, and inconsistencies are adjudicated.

- Enforcement: The mechanisms and level of oversight by which the objectives of the SoS capability to be delivered are ensured.

- Workforce: The examination of SoS workforce structures, unity of mission, and contract-based capability development.

- Incentive structure: The alignment between the enterprises goals and the incentive and reward structures of the individual stakeholders and stakeholder organizations that implement them.

- Knowledge ownership/access to knowledge: The accessibility of information regarding the operating environment, technical standards, and the other parts of the system-of-systems.

- Risk assessment/risk management: The degree to which risk assessment and management strategies are tailored to the specific risks of any one mission and the flexibility and resilience required for delivering SoS in the face of unforeseen developments.

After the initial data collection and processing phase, CSIS conducted a thorough examination and analysis of the interview results in Phase 2. During this phase, CSIS engaged various stakeholders and experts to assist in its analysis. This phase concluded with the submission of this project's first deliverable, a report outlining the key findings obtained through the interviews.

This report encompasses the final stage of the study. It brings together the information and data compiled in Phases 1 and 2 and presents a complete series of governance best practices in the field of SoS acquisitions. Detailed assessments

and analyses of selected case studies are provided and serve as examples of both successful and failed SoS capability development based on the eight identified CSIS attributes (see above). Here, CSIS uses its framework as a flexible tool to allow for uniformity in its analysis of all selected SoS case studies.

The aggregated results of this research illustrate how certain best practices in the three most critical attributes—level of organizational focus, decision-making authority, and enforcement—can make the difference between success and failure. Best practices in the remaining attributes also enable the efficient production and procurement of effective systems-of-systems, and assist mission success in large, complex acquisitions.

Current Approaches to Acquisition Governance and the Need for a New Model

The acceleration of technology innovation presents challenges for the traditional and time-tested acquisition practices of the DoD. In an effort to keep up, the DoD is engaging in acquisition projects and programs with increasing levels of complexity. In contrast to its traditional focus on individual technologies, the DoD uses complex systems-of-systems in order to ensure interoperability and take advantage of quick-moving technology areas in larger materiel projects with longer cycles.

Capabilities delivered as systems-of-systems are complex by definition. Among other attributes, this means they consist of multiple elements typically developed and managed by multiple organizations. Furthermore, their constituent elements frequently are part of multiple capabilities—a given system may be part of several systems-of-systems. This poses significant management and governance challenges.

Despite the difficulties inherent in complex acquisition, the payoff from successful delivery is the ability to achieve capabilities far greater than those provided by stand-alone complicated systems delivered by linear acquisition. The objective of the complex approach to acquisition is to allow the end-user community to reap the benefits of interoperable weapons and platforms and create capabilities multipliers through their interactions.

Success in complex acquisition is more than an exercise in systems engineering and technology integration. It requires good governance. Internally, governance is necessary to coordinate multiple work streams and deliver various sets of sub-systems and components each at a different stage of technological maturity. Governance is also critical to the management of a system-of-systems' interactions with other dynamic external systems, which not only inform the

technological and tactical operating environments in which the SoS capability is fielded, but also affect an SoS acquisition effort's resource availability and political feasibility.

Evolution of Acquisition Governance Models—Historical Context

Before defining complexity and outlining the factors that have contributed to its emergence, it is first important to establish historical context for defense acquisitions and the challenges inherent in acquisition efforts.

In the past, the government has responded to challenges in the acquisition environment by adjusting the division of responsibilities between itself, the customer, and industry suppliers. Harvey Sapolsky (2009) outlined various models of governance that the DoD has used in the past in a paper published by CSIS, titled "Models for Governing Large Systems Projects." Sapolsky (2009) suggested that the government has preferred to push more of the functional responsibilities of acquisition away from itself and toward industry contractors over time. This is in part a product of the flow of human capital toward the private sector and the erosion of the government's internal engineering expertise relative to industry. Although the elements of the Sapolsky model have different levels of analytic validity, the overall trends of skill and task migration from government to industry are well-documented and difficult to dispute.

The original model for weapons acquisition dates back to the earliest days of the U.S. defense infrastructure. At that time, the U.S. Navy could specify the warship it needed along with the design, construction, and outfitting of the ship. The Navy managed and performed production operations and generated technical requirements at all levels of the acquisition chain. Sapolsky (2009) titled this acquisition approach the "Arsenal Model," under which the government forms its own industrial base. It relies on scientists and engineers within the federal government's defense workforce. It is still employed to an extent today through the DoD's network of arsenals and maintenance depots around the country.

An acquisition approach known as the Contract Model involves greater industry participation in technical execution than the Arsenal Model. This model became dominant with the beginning of the Cold War. Increasingly, the government relied on the expertise and responsiveness of contractors to meet its needs for larger and more technically demanding weapon systems. Over time, the government maintained a workforce in contracting and acquisition program governance but began to outsource more technical execution to industry.

As weapons became more complex and management of these systems needed improvement, the acquisition community developed a preference for greater

industry involvement under the Weapon System Manager Model of acquisition. This model employs large contractors responsible for administration and coordination of a network of contractors working on subtasks integral to the overall acquisition effort. Passing responsibility to the weapon system managers has the advantage of involving large and responsive contractors that assist the integration of more complex systems that originate from a larger network of stakeholders.

As the DoD began to manage less of the implementation and fewer program management capabilities, it also started to lose its ability to provide technical direction for its acquisition efforts. This was accelerated by the end of the Cold War, when technical direction became almost exclusively the purview of industry. At this time, DoD leadership preserved combat capabilities while seeking savings within the technical functions of the services. This fourth model, known as the Outsourcing Model, grew more prevalent due to greater preference for private sector program implementation over government implementation.

The flow of more tasks and responsibility toward industry contributed to the growth of what Sapolsky (2009) called the "Lead System Integrator (LSI) Model" more commonly used today. Because LSI has been adopted to describe a specific type of contracting, this paper refers to Sapolsky's LSI Model as the "System Integration (SI) Model." In the SI Model, capabilities requirements are still controlled by military officers, but technical expertise is contracted to SIs to advance the capabilities of the planned weapon systems.

As the adaptation of Sapolsky's governance models in Table 2 indicates, the evolution of acquisition governance models over time—from preference toward the Arsenal Model in the earliest days of U.S. defense acquisition, to greater use of the SI Model in large weapon systems acquisition today—is characterized by the gradual removal of responsibility from the government buyer. In theory, moving all of the functions formerly performed by the government to industry contractors lessens the personnel burden associated with the maintenance of a large in-house acquisition workforce. Furthermore, reliance upon industry to designate technologies that meet warfighter demands is expected to facilitate the procurement and development of advanced capabilities in a shorter amount of time. However, this evolution has fallen short of expectations in practice and may instead be contributing to cost and schedule overruns and compromising the government's ability to manage large-scale acquisition efforts.

Table 2. Evolution of Acquisition Governance Models

Model → Task ↓	ARSENAL	CONTRACT	WEAPON SYSTEM MANAGER	OUTSOURCING TO PRIVATE ARSENAL	SYSTEM INTEGRATOR
PROGRAM REQUIREMENTS	Government	Government	Government	Government	Government/ Industry
TECHNICAL DIRECTION	Government	Government	Government	Industry	Industry
PROGRAM MANAGEMENT	Government	Government	Industry	Industry	Industry
TECHNICAL EXECUTION	Government	Industry	Industry	Industry	Industry
EXTERNAL ENVIRONMENT	Infrequent wars Little commercial application of military tech	Some commercial application of military tech Private sector pays better, can be more responsive	Weapons become more complicated /complex Coordination of sub-systems becomes important Large companies can leverage political support more effectively	Government begins to lose in-house tech capabilities Outsourcing becomes increasingly acceptable	Loss of in-house government tech capabilities leads to inability to define what's possible

Note. This table was adapted by CSIS from Sapolsky (2009).

The changing distribution of responsibilities between the industry supplier and the government customer, reflected in the Sapolsky model, serves to frame acquisition governance challenges in SoS acquisition. In addition, there are two distinct models for the direction of acquisition governance. In the traditional approach to acquisition governance, the capabilities comprising a system-of-systems are governed downward from the program-level. In an enterprise-wide governance approach, governance flows upward from the capabilities-level. Because the "enterprise approach" is an emerging model that is currently evolving to meet the demands of SoS complexity, its application is not evident in early-stage acquisition governance models. Instead, traditional, top-down approaches to acquisition governance have been most prevalent throughout the evolution of governance models, from the Arsenal Model at the dawn of U.S. armed services to the SI Model today.

Complexity—The Problem Defined

The existing governance models described above represent various ways to divide responsibility among customer and supplier stakeholders. These models illustrate how the DoD's preferences evolved to push human capital, technical knowledge, and production assets away from the government and toward industry.

However, these models fall short of providing an effective governance approach when faced with the challenges of complexity.

Within complexity theory, complex systems[1] are defined as those systems in which multiple components interact with, and exert influence on, one another and the various factors in their external environments over time. This research focuses on complexity within SoS acquisition specifically. Therefore, this paper uses *complexity* to describe systems consisting of multiple sub-systems and components that are typically developed and managed by more than one organization. The existing literature has applied the principles of complexity theory extensively to such fields as economics and business management.[2] This research aims to contribute to that body of literature by identifying best practices specific to the challenges defense and fed-civil acquisition managers confront in their SoS acquisition efforts. This focus is narrow, but as with other work that has been undertaken on complexity, its implications are applicable to other disciplines.

Complexity has emerged in major defense acquisitions for a number of reasons. The DoD has relied on systems-of-systems to facilitate the incorporation of quickly developing bleeding-edge technologies in large platforms, which tend to develop and reach production much more slowly. The rationale for complex SoS acquisition over more traditional approaches also originates in DoD's demand for more interoperable network operations and greater jointness among its constituent agencies and branches, as well as with international partners. Finally, acquisition leaders have invested in complex systems in order to create capabilities geared toward a broad range of both complementary and non-complementary requirements. In short, the level of complexity in DoD acquisitions has risen by default from the complexity of external systems (technology industries, threat environments, etc.), and by design out of the growing interest among defense planners to improve how well and in what ways the DoD satisfies its mission objectives.

Complex systems present four related problems for defense acquisition planners and decision-makers. First, the conceptual size of a complex system is larger than a traditional system. For example, ground vehicles used in the early- to mid-twentieth century were treated as one product; their interactions with other materiel were not negligible, but those interactions could be managed on a tactical level post-deployment. Conversely, today's ground vehicles contain their own sub-

---

[1] Much literature is dedicated specifically to complex adaptive systems, or CAS. These complex system are particular in that their sub-systems are able to respond to interactions and influences from other sub-systems and the external environment to protect the integrity of the system-of-systems. See, for example, Gell-Mann (1999). The complex systems discussed here do not assume that any system or sub-system is adaptive to its interactions or surroundings.

[2] For a discussion of how complexity theory has been applied in social and organizational sciences, see Levy (2000).

systems. A personnel carrier might have dozens of its own active and passive protection systems interacting with the vehicle and the external environment, a number of different communications devices, and various on-board weapons platforms, to name a few. Each of these systems has its own acquisition demands above and beyond the base requirements of the vehicle itself.

Second, each of the sub-systems within a system, as well as the systems external to it, interacts with others. Some of those interactions can be forecast to some degree, but forecasts will have limited accuracy. Furthermore, interactions can produce cascading interactions and change the behavior of other subsystems or the system as a whole. This contributes to a third problem complexity presents, namely that the output of a system is not equal to the sum of its inputs. The interactions can create amplified or diminished outcomes. This is a driver of complexity in defense platforms, as the multiplying effects of complementary systems can create new and more advanced defense technologies. However, as with the interactions themselves, it is difficult to forecast the individual and aggregate results of the system and sub-system interactions, much less to harness them for a desired outcome.

Finally, complexity is a problem because it operates outside the boundaries of traditional linear approaches to acquisition governance. This is central to objective of this report. Traditional, risk-averse governance approaches to designing, engineering, developing, and procuring defense weapons and platforms are not adequately flexible to manage the unpredictable interactions of systems, sub-systems, and the external environment. They create static program objectives to acquire dynamic technologies. Those technologies often evolve at widely different rates of development, and upgrading platforms with long life cycles can be difficult.

Existing Governance Models Are Too Rigid for Complex Acquisition

The inability of existing governance models to manage complex acquisitions effectively is apparent in the pervasive process challenges the DoD faces, as well as the poor outcomes of major acquisition efforts. Both of these factors are core indicators of the effectiveness of governance. *Process* is used here to refer to the collective operational inputs the government employs in executing projects and programs—labor inputs, bureaucratic requirements, and so forth. *Outcome* describes the products or services governance processes deliver, the time and cost required to deliver those products or services, and the alignment between the time and cost objectives and actual time and cost results.

Workforce capacity and organizational hierarchy are two areas of process strain in the existing governance structure. As capabilities become more complex, they demand a DoD systems engineering workforce that may exceed what the

government customer can offer. Additionally, the pace of project execution under traditional approaches to acquisition, along with the centralization of decision-making autonomy in government branches—especially in the DoD—frustrates project and program managers' ability to respond to resource challenges and manage operations autonomously.

These process challenges can result in structural difficulties for SoS capabilities that may not exist in traditional acquisition approaches. For instance, knowledge-sharing—a straightforward task in traditional acquisition—faces new challenges in complex SoS acquisition efforts. Knowledge ownership and incentives for sharing become less clear, adding to the host of governance process shortfalls. Compounding these challenges in technology, operational requirements, and structure, the DoD organizations needed to develop and deploy the SoS capabilities are bigger and more difficult to manage and maintain than traditional acquisition organizations, particularly under the SI Model.

The growing divide between acquisition governance models and acquisition in practice is also clear in SoS acquisition outcomes. Government customers' ability to deliver complex SoS capabilities on cost in particular is declining. According to the Government Accountability Office (GAO, 2013), more than 86 MDAPs in fiscal year 2012 showed approximately $400 billion in aggregated cost overruns since their first full-year estimates, representing a 4% ($90 billion) growth in development costs and a 5% ($290 billion) growth in costs of procurement. As dramatic as this cost growth is, this latest annual report from the GAO is actually anomalous when compared against even greater cost growth in the 2012 report. In that iteration, 96 MDAPs existing in that year had grown an aggregated $447 billion in excess of their original estimated costs (GAO, 2012). Given the expected impact of sequestration, the 2012 report is likely to more accurately represent the trend in cost growth. That trend is particularly evident when compared with the 2007 GAO report, which cited 64 MDAPs in the DoD's accounts that had grown at an average annual rate of 4.9 percent. This produced a total annual cost growth of $165 billion by those programs in that year (GAO, 2007a). This indicates that cost overruns grew 170.9% in the years between 2006 and 2011.

The government is also encountering challenges in keeping its major weapons programs on schedule. In its latest report, the GAO (2013) found that MDAPs experienced an average delay of 27 months in reaching initial operational capability. This figure exceeds the 2012 estimate of 23 months in average delay. Combined with the upward trend in cost growth over time, this track record indicates that existing governance and management tools no longer suffice for today's complex weapon systems.

As cost and schedule overrun trends illustrate, delivering systems-of-systems depends on getting governance right. However, the traditional service-centric approach to acquisition governance is not sufficiently flexible to meet the needs of systems-of-systems. Specifically, flexibility is limited in two ways.

First, the current process of generating requirements does not allow for the integration of changes in user needs. Because complex systems-of-systems are inherently dynamic, non-linear, and risk-intensive, acquisition leadership's ability to react to changes in user needs is critical to the successful delivery of SoS capabilities. Structured but flexible oversight procedures improve alignment between DoD requirements and fielded systems by establishing clear systems-level metrics and measuring progress toward declared goals. Systems must also be able to respond to changes in external factors in order to ensure that the SoS capability is as relevant when it reaches the production and deployment phase as it was in pre-acquisition phases. These factors could include macro-level changes in the security environment and technological advances, as well as micro-level changes in organizational politics and acquisition effort leadership.

Second, successful acquisition delivery requires the "power of the purse" to direct solutions and approaches. In order to direct efforts toward certain capabilities, program leadership must be able to dedicate resources such as real contracting dollars, as well as human capital and allocations for other overhead costs, to certain system efforts. However, budgetary power is limited when individual services and defense agencies are the highest level of governance, due to the relatively more limited ability of those stakeholders to guarantee funds for the system or to be able to shift and reapportion them at the system-level. The process by which funds are secured also limits flexibility; the DoD's 20-month-plus budget cycle that precedes actual appropriation may lead the DoD to acquire technologies that are bleeding-edge when a budget is begun but that may become outdated by the time the budget is enacted.

The root causes of limited flexibility in SoS acquisition efforts are themselves complex and reflect a variety of challenges. One major theme of problems is the division of authority at different levels of an acquiring organization. Systems reside in different programs that are designed, funded, managed, and implemented by different entities. Another problem with this lack of necessary authority is that no entity below the under secretary of defense for acquisition, technology, and logistics (hereafter, the USD[AT&L]) can make SoS decisions, which is especially important regarding the synchronization of capabilities across sub-systems. Other issues pertaining to the lack of necessary authority include the inadequate oversight and enforcement at the SoS level, in addition to the limited organizational ability to coordinate across schedule, funding, and technical areas.

Two other major themes of root causes are the lack of warfighter input and the need for DoD processes to change. Iterative warfighter input, particularly as it relates to end-user requirements, is insufficiently integrated into systems-of-systems. Many systems-of-systems possess a disconnect from warfighters' needs even after SoS integration. Current DoD processes mirror the governance model that is stovepiped in the services and agencies that authority, budgeting, and implementation occur. These processes are geared toward delivery of hardware programs and not optimized for delivery of systems-of-systems, capabilities, or services. Many of these processes also underestimate the cost and complexity of a system-of-systems.

Other major themes underscoring the root causes of ineffective governance include poor risk assessment and management, requirements prioritization, and communication. Risks are often not addressed beyond systems level and are often underestimated in their original assessments. These unrealistic assessments cause synchronization difficulties, which affect risk management later during implementation. Prioritization of requirements is another major theme in the root causes as requirements, which are often ambitious, are not resource constrained, and are subject to frequent changes, often leading to cost and schedule problems. In addition, the inefficient requirements process often produces programmatic synchronization problems. The last major theme that deals with root causes is communication. Insufficient communication occurs both internally and externally. For program leads, insufficient notification on cost and schedule slippages between programs often leads to distrust and inefficiencies. For end-users, insufficient communication on cost, schedule, and requirements also causes distrust and inefficiencies.

Enterprise-Wide Governance Is Key to Success in Complex Acquisition

Given the limited effectiveness of traditional service-centric approaches to governance in dealing with complexity, it is useful to look at new, enterprise-wide governance models for the acquisition and delivery of complex SoS capabilities.

Numerous platforms and systems comprise a system-of-systems, and the interactions of these components are highly unpredictable. Coordination of these internal constituent systems is necessary to achieve the desired SoS capability, which otherwise would be out of reach for any single component alone. CSIS research suggests an enterprise-wide approach to governance would facilitate oversight and accountability of the systems' individual components to achieve that coordination.

Problems associated with a service-centric approach to governance appear to originate in their limited resource and decision-making agility. Successful delivery of systems-of-systems depends on the ability to react to changes in user needs, external factors (including the global security environment and organizational politics), and technological progress. Most of all, it requires the power of the purse to direct solutions and approaches. But such power is nonexistent when individual services and agencies are the highest level of governance, and rapid reaction is difficult given the DoD's 20-month-plus budget cycle and the six to 24 months needed to get through the requirements cycle.

Outdated oversight mechanisms also contribute to process burdens in complex acquisition and negatively impact the outcomes of large DoD programs. The traditional approach to acquisition is geared toward more traditional, linear acquisition programs. Existing models were not designed to organize a diverse set of stakeholders around a common mission. While the DoD has attempted to bring new thinking to systems engineering to tackle some of the challenges of complexity, program management thinking remains stuck. By applying cumbersome, rigid oversight processes, the DoD has slowed the pace of its advanced technology innovation efforts and lessened its ability to realize the benefits of complex SoS acquisition.

Developing new governance models requires a better understanding of program attributes (i.e., what the program needs in order to succeed) and of the elements of governance that different organizations possess. On the program side, additional research is needed on how funding stability, schedule stability, technology maturity, stability of requirements, estimated versus contracted cost, and management stability affect performance. On the organizational side, attributes such as technical awareness, project management skill, customer understanding, organizational longevity, manufacturing expertise, and organizational independence require more attention. That said, the existing governance and management tools no longer suffice for today's complex programs.

The results of CSIS research indicate that an enterprise-wide approach to governance may improve the DoD's ability to understand complex acquisition efforts. Because complex systems-of-systems are inherently dynamic, non-linear, and risk-intensive, they require clear directional leadership from the top. However, complex acquisition efforts and the organizations designed to manage them must also exhibit agile resource utilization from below. The enterprise model discussed in this paper features several attributes that CSIS research suggests contribute to resource agility.

In contrast to the highly linear traditional model of governance, the enterprise model encourages broad and flexible authority delegation. The case studies

illustrate that this feature, when paired with effective directional leadership in the form of standards and review processes, allows stakeholders with different functions at different levels of the organizational hierarchy to more closely interact with one another and more effectively respond to changes in external systems, especially the complex system comprised of various environmental factors.

An additional feature of the enterprise model that makes it ideal for describing the governance of complex systems is that it is more easily adapted to the requirements of specific organizational goals. Research illustrates that a one-size-fits-all policy or model is not appropriate for the challenges of complexity. Literature on the application of complex systems theory to organizational design is nearly unanimous in its emphasis on informal hierarchies as opposed to global, rigid structures such as those encouraged by existing DoD 5000-series acquisition guidelines.

Systems-of-Systems Acquisition Case Studies

As discussed in the previous section, there is a need for a new model of governance in DoD efforts to develop and procure complex systems-of-systems. This section describes seven cases of complex acquisition, each with unique process challenges and outcomes. It presents research on these cases based on secondary data as well as interviews with program executives and leaders in the acquisition community. Each case is shown to have managed complexity to various levels of success and with different resource demands based in part on its performance in eight attributes of governance.

CSIS notes that the analysis, findings, and conclusions of each of these case studies are entirely the product of CSIS research and may not be consistent with or reflect official government assessments of or data from the programs themselves.

Overview

CSIS developed its framework for analysis of governance in complex acquisitions through previous work on SoS governance. The framework is the product of research on SoS governance models, interviews with program stakeholders and industry leaders, and a findings refinement process involving input from SoS experts. It consists of eight attributes that collectively represent concerns, questions, and issues that must be addressed for an organization to succeed in acquiring a complex system-of-systems. The importance and significance of these attributes varies depending on the system to which the framework is being applied.

The eight governance attributes are as follows:

- <u>Level of organizational focus:</u> The level at which SoS governance occurs within the organization. This is not the same as

systems/capabilities focus or technical focus, both of which are outside the scope of the CSIS SoS governance analysis.

- Integration of functional end-user needs: The mechanisms and frequency with which the functional needs of end-users are built into the system-of-systems, and at which points in the process this incorporation occurs.

- Decision-making authority: The governance mechanisms for SoS delivery, including how budget is allocated, standards are set, tradeoffs are managed, and inconsistencies are adjudicated.

- Enforcement: The mechanisms and level of oversight by which the objectives of the SoS capability to be delivered are ensured.

- Workforce: The examination of SoS workforce structures, unity of mission, and capability development through use of contracting.

- Incentive structure: The alignment between the enterprise's goals and the incentive and reward structures of the stakeholders and organizations that implement them.

- Knowledge ownership/access to knowledge: The accessibility of information regarding the operating environment, technical standards, and the other parts of the system-of-systems.

- Risk assessment/risk management: Risk assessments and management strategies tailored to the mission accomplishment and the flexibility and resilience required for delivering systems-of-systems in the face of unforeseen developments.

CSIS has examined relevant case studies to better understand how these eight attributes affect programs. This section assesses and analyzes these selected case studies based on the eight CSIS attributes above to serve as examples of both successful and failed SoS capability developments. The application of the eight-attribute framework will serve as a flexible tool for consistent analysis of all selected SoS case studies. Case studies examined are presented in Table 3.

Table 3.   The Center for Strategic and International Studies SoS Governance Case Study Programs

Traditional Governance	Enterprise Governance
• Future Combat System (FCS) • Integrated Deepwater System (Deepwater)	• Counter Rocket, Artillery, and Mortar (C-RAM) • Distributed Common Ground System (DCGS) • Global Nuclear Detection System (GNDS) • Harvest Hawk • Maritime Domain Awareness (MDA)

These case studies are presented in alphabetical order, beginning with those programs that fall in the traditional model category. Each case study provides an overview of the program objectives, specifics about lead agency(ies) acquisition strategies, and a brief discussion of the program's successes and failures. Most importantly, each case study presents an analysis of program characteristics with reference to the eight governance attributes.

Frameworks Versus Models: From Conceptual to Concrete

The traditional and enterprise models describe two ways to conceptualize a complex SoS effort, but they are insufficient in themselves to describe best practices in SoS governance. Instead, the models discussed in this research represent two paths of logic for understanding complexity. The traditional model represents linear logic. Scholarship on complexity shows that this kind of logic contributes to difficulty in understanding and dealing with complexity.[3] The enterprise model, as applied here, incorporates the individual elements of acquisition efforts and organizes them in a non-linear way. Acquisition managers can use this model to visualize and analyze the relationship of each element to other elements. The next section illustrates how this approach contributes to more agile governance.

The models are valuable only insofar as they represent two ways in which acquisition leaders can conceptualize their acquisition efforts within the context of complexity. A more concrete set of tools is necessary to organize acquisitions into concrete variables that can be analyzed historically and controlled in future efforts.

---

[3] In his book on complexity in military operations, Edward Smith (2006) wrote, "The reality is that dealing with the complexity is not difficult. … Rather, our difficulty stems from trying to deal with the *non*linearity of our complex security environment using only linear logic, metrics, and thinking" (p. 66). This concept provides the basis for much of the scholarship on applications of complexity theory to economics and business management. Smith's (2006) position is also echoed by literature on related theoretical frameworks, such as constructal theory, network theory, and chaos theory.

This research uses the CSIS acquisition governance framework to accomplish the task of turning case analysis into concrete, functional best practices. Whereas the categorization of each case as either an enterprise approach or a traditional approach facilitates the conceptualization of complexity, the CSIS governance framework provides the necessary tools for dealing with it. By breaking down governance into key controllable components, the framework enables analysis of specific best practices to support mission success in complex acquisition efforts.

Traditional Model Case Studies

In the traditional approach to acquisition governance, a program office or a similar central authority mandates and governs the capabilities comprising a system-of-systems. Linear acquisition activities follow defined user needs, typically in the form of broad tactical requirements. The acquisition activities begin with overarching technical requirements, which inform bids from government and industry suppliers. Program offices analyze bids for their closeness-of-fit to certain criteria and select a winning solution. The winning contractor then develops, produces, and deploys the system-of-systems (see Figure 1).
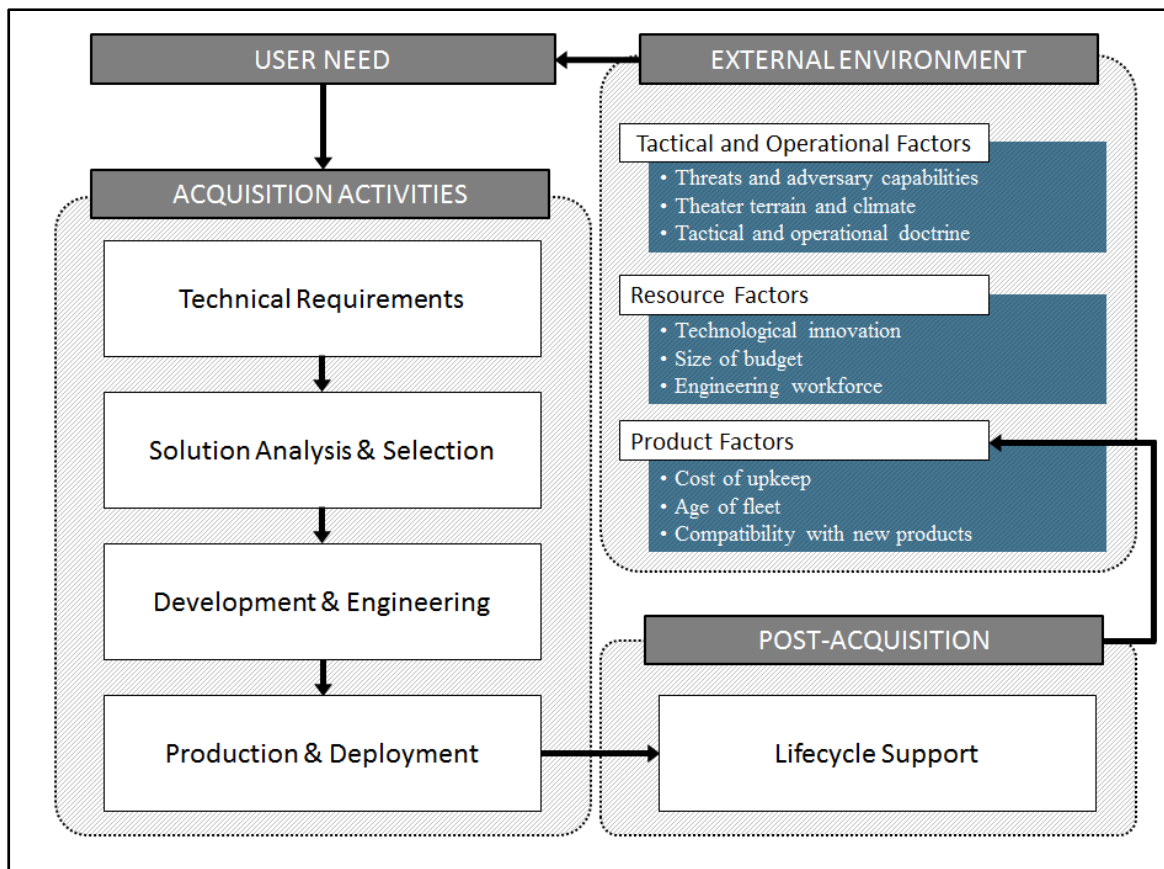
Figure 1.   Traditional Acquisition Governance

Note. This figure comes from CSIS analysis. "Acquisition Activities" was adapted from standard defense acquisition protocols, as outlined in DoD (2008, p. 12).

As illustrated in Figure 1, the traditional model of acquisition governance has a linear form. The nature of inputs determines the output at any single stage in this model. The user needs to trigger a standardized acquisition process. The customer operates and maintains that product over its life cycle. The ability of the product to meet changing needs, along with other changes in the external environment, is limited. Those dynamics instead influence new user needs, or early-stage user needs being used to drive acquisition activities, which in turn result in a new round of acquisition.

Linearity in an organization creates problems when the organization encounters the challenges of complexity. Without meaningful authority of its own, a lower-tier component of the acquisition hierarchy is forced to defer to higher levels of the linear organizational structure. As the case studies presented here illustrate, these long authority chains strain the ability of personnel to create new and innovative ways to solve external challenges. They also slow the process of

acquisition and widen the gap between time to product delivery and rate of new capabilities development in the external environment (i.e., private sector).

The case studies identify three interrelated ways in which the linearity of the traditional model challenges the ability of the DoD to execute complex SoS efforts and to deliver capabilities on-cost and on-schedule. First, individual stages of the acquisition process have difficulty responding to changes in user needs and the external environment once these inputs have set the technical requirements. Second, efforts to preempt changes in those inputs often result in acquisitions of immature technologies with high levels of risk. Finally, as delays occur in the development of components of the systems, parent systems cannot adapt which creates setbacks. This effect can occur in any complex effort regardless of the model, but the structure of the traditional model of governance exaggerates this effect.

CSIS analysis shows that the cases in which the traditional model of governance was applied were slow to react to changes in the environment and the evolution of new user needs. Formal, top-down authority and long-term planning caused fatal problems to emerge in both cases and encouraged numerous restructuring efforts. Finally, while executives in the acquisition cases had tried unique approaches to managing complexity, they were restricted by existing policy frameworks and acquisition guidelines into more rigid governance structures.

Future Combat Systems

Future Combat Systems (FCSs) was conceived as one of three substantial initiatives to modernize the Army. After nine years of development and with a project total cost of $200 billion, the Army terminated the program. The challenges FCS faced and the eventual cancellation of the program illustrate the importance of planning for system interdependency and exercising strong enforcement mechanisms to deliver large SoS capabilities.

The FCS program was officially initiated with a four-team competition in February 2000 and terminated nine years later in 2009. It initially consisted of 18 manned and unmanned systems linked together via a network. As the largest acquisition program ever attempted by the Army, FCS was envisioned to transform the service by replacing current systems such as the M-1 Abrams tank and the M-2 Bradley infantry fighting vehicle as well as by adding new capabilities.

Table 4.   Future Combat System Governance Attributes

Governance Attributes	Program Characteristics
Level of organizational focus	• Narrow, program-level focus • Program managers paid little attention to enterprise components with which FCS was supposed to integrate (namely WIN-T and JTRS)
Integration of functional end-user needs	• Top-down requirements-setting based on Army Vision (1999) and Mission Needs Statement (2000) documents produced low integration of end-user needs into ongoing FCS development • Although mechanisms were present to integrate changing requirements, there is little evidence that they were used
Decision-making authority	• Program organized to segregate decision-making and push it downward o 7 SoS Integrated Product Teams (IPT) and 7 Systems product teams established to provide product and process oversight • Authority became concentrated at the Program Manager level, as the key component of the relationships between the LSI and oversight offices
Enforcement	• OSD oversight officials required revised baselines in Milestone B approval due to unacceptably high costs and risks, but Army's reintegration of original baselines after the fact point to weak enforcement mechanisms
Workforce	• Contractor program managers act in the role of acquisition leadership • IPTs (product and mission offices) co-led by one appointee from the LSI, and one appointee from the Army
Incentive structure	• Performance incentives based on completion of program events (design reviews, etc.) rather than product performance • Cost incentives based on projected life-cycle cost

Knowledge ownership/ access to knowledge	• FCS exhibits significant problems with stovepiping of knowledge
	  o Sub-contractors were hesitant to submit competitive information to the Boeing-SAIC LSI team
	  o Other Transaction Agreement- (OTA) based contract limited the amount of knowledge the LSI was required to share initially

Risk assessment/risk management	• PM FCS and Boeing-SAIC conducted independent assessments of the FCS health periodically using Earned Value Management System (EVMS) • Many of the technologies selected for FCS were developmental and at low levels of maturity, and could not be monitored with hard metrics

Note. This table comes from CSIS analysis.

The concept for FCS emerged out of a joint study proposed in 1999 by General Paul J. Kern, then the military deputy to the assistant secretary of the Army for research, development, and acquisition. Gen. Kern proposed to the Defense Advanced Research Projects Agency (DARPA) a study on the future Army. The study advisory group found that in order to achieve Kern's vision—to be mobile, lethal, survivable, and responsive—the Army needed a system-of-systems (Gorman & Diehl, 2003, p. B-11).

In May 2000, DARPA awarded four contracts to four industry teams to develop FCS designs. The Army awarded the lead systems integrator (LSI) contract to a Boeing and Science Applications International Corporation (SAIC) team in March 2002 after nearly two years of design evaluation. The Boeing and SAIC team worked with more than 550 contractors and subcontractors in 41 states.

In its earliest stages, the Army planned to build FCS with 18 systems, all linked by a single network. In May 2003, the Office of the Secretary of Defense for

Acquisitions, Technology, and Logistics (OSD[AT&L]) required the Army to cut several systems in order to receive Milestone B approval. The Army reduced the total number of systems to 13. However, the Army reintegrated the cancelled systems back into FCS two years later when it conducted a re-baselining of the program in November 2005 (Pernin et al., 2002; see Table 5).

Table 5.   Adjustments to FCS Family at Key Program Points

#	System	Acronym	2003	2005	2007
1	Mounted Combat System	MCS	X	X	X
2	Infantry Carrier Vehicle	ICV	X	X	X
3	Non Line of Sight Cannon	NLOS-C	X	X	X
4	Non Line of Sight Mortar	NLOS-M	X	X	X
5	Command and Control Vehicle	C2V	X	X	X
6	Reconnaissance and Recovery Vehicle	RSV	X	X	X
7	Maintenance and Recovery Vehicle	M&RV		X	X
8	Medical Vehicle	MV	X	X	X
9	UAV Class I	UAV-CL1	X	X	X
10	UAV Class II	UAV-CL2		X	
11	UAV Class III	UAV-CL3		X	
12	UAV Class IV	UAV-CL4	X	X	X
13	Armed Robotic Vehicle			X	X	X
14	Multifunctional Utility/Logistics and Equipment	MULE	X	X	X
15	Non Line of Sight Launch System	NLOS-LS	X	X	X
16	Small Unmanned Ground Vehicle	SUGV	X	X	X
17	Intelligent Munition Systems	IMS		X	
18	Unmanned Ground Sensor	UGS	X	X	X

Note. This table was adapted by CSIS from Pernin et al. (2002).

At the outset, the FCS family of capabilities was expected to enable a warfighter to assess the battlefield and control response capabilities from a manned command and control vehicle, the C2V. The vehicle would access and command other assets through the through the central network. The GAO reported in 2001 that the success of this concept would depend in part "upon mature technologies to allow the Army to design secure networks that cannot be jammed or taken over by the opponent" (p. 6).

Throughout much of its existence as a PoR, FCS attracted intense scrutiny. For example, the National Defense Authorization Act (NDAA) for Fiscal Year 2006 mandated that "[the] Comptroller General shall conduct an annual review of [FCS] and shall, not later than March 15 of each year, submit to Congress a report on the results of the most recent review." The NDAA designated certain items to be included in that report, with a focus on (1) systems development and demonstration goals and progress; (2) budget for current and next fiscal year for all DoD programs supporting FCS; (3) plan for systems development and demonstration; and (4) the comptroller general's conclusion on whether the development and demonstration of supporting systems is likely to be completed at a total cost not in excess of the amount specified in the Selected Acquisition Report for FCS.

The low maturity of FCS component technologies was a significant source of problems in systems integration and created substantial risk for the program. Delays in component technologies also had a cascading effect through the entire FCS enterprise. A GAO report dated March 2007 notes that one best practice in knowledge-based acquisition is to have all critical technologies matured to technology readiness level (TRL) 7 by the product development phase. However, "even with the progress the program has made in the last year, fewer than 35 of FCS's 46 technologies have attained a lower maturity—TRL 6—3½ years after starting product development" (GAO, 2007b). The substantial degree of interdependency between and among the systems also created a situation in which developers could not test components before the completion of the system-of-systems as a whole, which made low technological maturity particularly dangerous.

FCS also lacked risk management mechanisms to handle the challenges of inconsistent maturity across component technologies. One source observed that Army officials were still developing risk mitigation plans as late as April 2004, about five years after the start of program's early stages (Kwak & Smith, 2009). One interviewee noted absent specific risk mitigation plans and that FCS program management used DAU risk management methodology that was not suitable for the governance of cascading technology failures. Combined with the lack of alignment on the FCS vision and management between enterprise-level overseers, such as OSD(AT&L) and their counterparts in the Army and at the FCS program office, the lack of effective risk management contributed to cost growth and schedule slippage. At the time of its cancellation, the total cost for FCS had ballooned from initial estimates of $99 billion to a projected $200 billion (Cornin, 2012).

Finally, programmatic problems also contributed to the failure of FCS. First, the capabilities in the design of the program had fallen out of alignment with the warfighter's needs. Most notably, the manned ground vehicle (MGV) portion of the program in particular was not suited to the close-combat and urban terrain operations in which the Army was engaged. A second problem with the program was the shortfall of remaining resources compared with the level of progress achieved. By the time of the Preliminary Design Review, the program had consumed 60% of its funding, which left the remaining portion to cover the entire systems development phase.

These technical, risk-related, and programmatic problems suggest that a narrow level of focus at the program level rather than at the level of the enterprise can erode the value of a program and commitment to its completion. Although discussions at the program manager level touched upon integration with other Army programs, the details of integration remained unclear and the program operated in a virtual vacuum. Combined with the low alignment of end-user needs with the

capabilities the program promised, this level of focus created an environment in which the Army was unable to defend against scrutiny of the challenges brought about by the complexity of the acquisition effort.

Most importantly, the program's failure demonstrates that enforcement is a critical governance attribute. The level of technical maturity at early stages of an acquisition—especially during solutions analysis and source selection—greatly influences the degree to which enforcement is needed and the level of strength and formality in enforcement mechanisms. In the case of FCS, enforcement existed formally through the DoD 5000-series milestones but does not appear to have been strong enough.

Integrated Deepwater System

The Integrated Deepwater System (Deepwater) acquisition program began as a comprehensive effort to modernize the Coast Guard's fleet of aviation and maritime surface assets, and link them through a sophisticated Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) network. The ambitious recapitalization plan encountered problems primarily in its inability to align a diverse set of competing interests. In 2012, the program was broken into 13 major acquisition efforts. The Coast Guard's struggle to integrate all of its recapitalization requirements into one formal program illustrates that top-down, components-focused governance is ineffective in accomplishing complex acquisition.

Table 6.   Integrated Deepwater System Governance Attributes

Governance Attributes	Program Characteristics
Level of organizational focus	• Initially managed at the program-level with limited overarching leadership • From 2009, USCG installed an Executive Oversight Council (EOC) to offer programmatic guidance at the enterprise level • As of 2012, the Deepwater effort spans 13 major programs
Integration of functional end-user needs	• Large materiel procurement efforts did not respond to changing end-user needs in a timely manner • Some asset-level procurement decisions did not correspond with program requirements established at the enterprise level

Decision-making authority	• Nearly all decision-making was delegated to the LSI prior to program transition in 2007
	  o The LSI contractor issued Request for Information (RFI) and Request for Proposal (RFP) documents, in addition to handling new contracts through a subcontracting mechanism
	• Today, EOC discusses and coordinates program-level decisions
	  o EOC chaired by Acquisition Directorate with executives from each of the other USCG directorates

Enforcement	• Funding was insufficient to allow on-time delivery of components critical to the enterprise-level systems • The LSI was held accountable for technical failures through an audit process and the threat of recompetition
Workforce	• LSI contractor workforce did not have substantial experience in implementing acquisition logistics, causing effort redundancies and compounding problems with insufficient funding • Reliance on LSI contractor for "cradle-to-grave" management of Deepwater left USCG with an insufficient acquisition workforce
Incentive structure	• USCG negotiated change order terms and set positive contract incentives in its contract with ICGS, the Deepwater LSI contractor
Knowledge ownership/ access to knowledge	• Deepwater at times lacked dedication of USCG leadership in facilitating both access to and use of information among stakeholders
Risk assessment/risk management	• USCG's risk management model primarily focused on ensuring technologies of interest were at an appropriate technological readiness level • Standards-based acquisition approach pursued "Plug-and-play" technologies for C4 systems

Note. This table comes from CSIS analysis.

Deepwater was planned as a two-decade effort to replace 206 aircraft and 93 cutter ships. The USCG designed and executed a transformational SoS acquisition approach to the program in order to ensure the air, surface, and C4ISR assets procured under Deepwater would be integrated and interoperable.

The program began in 1998 with a RFP for Phase I study that attracted bids from three industry teams (Warwick, 1998). In June 2002, the USCG awarded an $11 billion LSI contract to Integrated Coast Guard Systems (ICGS), a joint venture between Lockheed Martin and Northrop Grumman formed for the Deepwater competition (Koch, 2002). Under the terms of this contract, ICGS was tasked to

oversee all asset procurement activities, systems integration operations, and program management duties.

The Coast Guard planned for Deepwater to accomplish a complete recapitalization of its aging fleet of air and surface assets. The Coast Guard's decision to approach recapitalization as a system-of-systems was based on the belief that the effort could be executed in a more cost-effective manner if all Deepwater-capable assets were acquired as one integrated package (O'Rourke, 2011). The result was a single program led by an industry LSI for the acquisition of various quantities of 14 major platforms and several networks and logistics components (O'Rourke, 2011, pp. 4–5). Those sub-systems are shown in Table 7.

Table 7.   Planned Acquisitions for Deepwater (2006 Baseline)

#	System	Quantity	Cost ($M)
1	HC-130J Long-Range Surveillance (LRS) aircraft	6	**11**
2	HC-130H LRS aircraft	16	**610**
3	HC0144A Medium-Range Surveillance (MRS) aircraft	36	**1,706**
4	MH-60T Medium-Range Recover (MRR) helicopters	42	**451**
5	HH-65C Multi-Mission Cutter Helicopters (MCHs)	102	**741**
6	Vertical take-off unmanned aerial vehicles (VUAVs)	45	**503**
7	National Security Cutters (NSCs)	8	**3,450**
8	Offshore Patrol Cutters (OPCs)	25	**8,098**
9	Fast Response Cutters-Class A (FRC-A)	46	**2,613**
10	Fast Response Cutters-Class B (FRC-B)	12	**593**
11	Medium Endurance Cutters (MECs) upgraded with Mission Effectiveness Project (MEP)	27	**317**
12	Patrol Boats (PBs) upgraded with MEP	17	**117**
13	Small boats for Deepwater cutters	124	**110**
14	110-foot Island-class PBs converted into 123-foot PBs	8	**95**

Note. This table was adapted by CSIS from O'Rourke (2011, pp. 4–5).

Although Deepwater initially garnered praise from policy-makers and stakeholders within the government and industry for its innovative approach to acquisition, the program encountered several problems in its execution. Funding came at a rate that was slower than the service had anticipated, causing program delays (Hughes, 2003). Enterprise-level requirements were at odds with asset-level requirements in at least one high-profile acquisition effort.[4] Finally, USCG also had difficulties incorporating new and changing requirements into Deepwater, especially as the service began executing more homeland security missions in the wake of the terrorist attacks of September 11, 2001.

These difficulties, combined with the USCG's inability to secure sufficient accountability from its LSI contractor, eventually led to the dissolution of the LSI-led

---

[4] Media sources indicate an effort to overhaul the HH-65 Dolphin engine did not take into account the Deepwater requirements on engine certification (see "Honeywell Has Filed," 2004).

acquisition approach. USCG indicated in July 2007 that it would assume the integrator role and implement a transition to a model in which asset-level procurement is integrated through enterprise-level, government-led governance (Geoff, 2009).

The USCG completed its transition of the Deepwater program in 2012 when it split the program into 13 separate programs. In its FY 2012 budget request, the Coast Guard proposed scrapping the term "Deepwater" to refer to the asset acquisition effort. This reflects the Coast Guard's view that the fleet is a system-of-systems for the purposes of integration across the Coast Guard as a whole, but not for the purposes of acquisition (O'Rourke, 2012, p. 3).

Enterprise Model Case Studies

The enterprise model of acquisition governance breaks SoS acquisition into different layers of authority. This characteristic is a key difference between the enterprise model and the traditional model, which employs a top-down unified approach to governance. The division of authority allows different stages of an SoS acquisition effort to influence one another in separate bilateral relationships. It also enables individual stages of acquisition to adapt to changes in the external environment. These characteristics comprise a more agile approach to acquisition (see Figure 2).
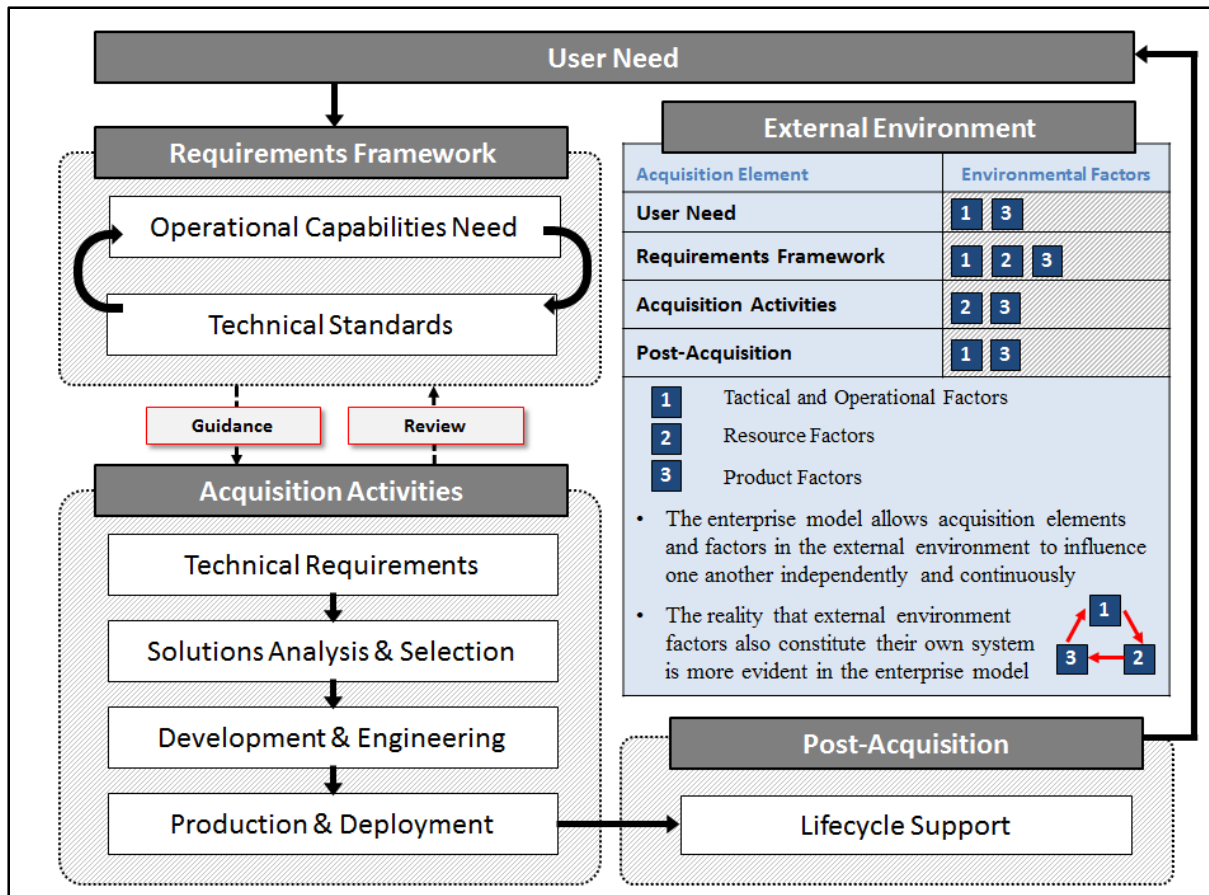
Figure 2. Enterprise Acquisition Governance
Note. This figure comes from CSIS analysis.

The enterprise model of acquisition governance illustrates that the enterprise approach separates general program requirements from sub-system technical requirements. This important feature of the enterprise model allows sub-system customers the freedom to generate technical requirements specific to their own needs while ensuring compatibility and interoperability with the parent system. It also promotes standards-based acquisition and open-source, open-architecture technology development at the components level. Collectively, these benefits help the acquisition community adjust to quickly changing end-user needs and new technology developments while maintaining SoS objectives set at the enterprise level.

The enterprise model's layered authorities also alter the relationship between the environment and other elements in the model's ecosystem. As illustrated by Figure 1 in the previous section, the traditional model treats the external environment as its own unit. This allows environmental factors to inform user needs but makes it more difficult for them to influence other stages of the acquisition effort. For example, resource factors are critical to solutions analysis and selection;

however, aside from the influence resource factors exert in the initial stages of solutions analysis, top-down governance in the traditional model complicates real-time adjustment to changes in those factors.

The relationship between the acquisition organization and the external environment has a material effect on how acquisition efforts are executed and what outcomes they reach. Research on the application of complexity theory to organizational design shows that sensitivity to environmental dynamics is critical to the effectiveness of product- and innovation-focused organizations, such as the organizations created to govern individual DoD acquisition efforts (see Maxfield, 1997). When an organization is not adequately responsive to changes in the external environment, relationships among the internal acquisition elements become strained and destabilize.[5] In instances where the enterprise model features directional leadership—as opposed to top-down, prescriptive leadership—research indicates the model allows for different environmental factors to influence governance at each acquisition element through the element's localized authority.

It is important to note in analysis of the enterprise model that the external environment is also a complex system in itself. Changes in the environment comprise a second dimension of complexity known in business management parlance as "turbulence." As opposed to the traditional model, which tends to direct environmental variables as a whole toward the top of the authority chain, the enterprise model facilitates observation of changes in individual factors within the external environment and the turbulence that results from their interactions. For example, acquisition personnel and decision-makers can more readily observe the impact of a change in operating environment from desert to wetlands—a change in operational factors—on the cost of upkeep for a land vehicle—a product factor. This dynamic is captured in the "External Environment" section of Figure 2.

As this discussion indicates, layered authority is the key differentiator of the enterprise and traditional models. However, the case studies presented here suggest that the acquisition community has been selective about how it divides authority even in those efforts most representative of the enterprise model. This is where the CSIS eight-attribute governance framework is particularly important. This research uses the framework to observe how individual attributes relate to each case's ability to manage complexity internally and externally. The cases show that the ability to manage complexity directly correlates with the degree to which the responsible stakeholders have independent authority in each attribute for which they are accountable.

---

[5] Research on complexity in business management concepts and strategy formulation has explored these relationships in detail. See, for example, Roger Mason's (2007) "The External Environment's Effect on Management and Strategy: A Complexity Theory Approach."

The case studies also illustrate that the enterprise model has not been applied uniformly to any single acquisition effort. Rather, leaders in the acquisition community use best-practices encompassed by individual bilateral relationships between different layers of authority to achieve specific program goals. For example, the Distributed Common Ground System (DCGS) program utilizes a bilateral relationship between requirements framework and acquisition activities to ensure that technical requirements for new sub-systems meet the technical standards of the system-of-systems and satisfy its capabilities requirements. Maritime Domain Awareness, a Navy-led cross-government effort, has kept its requirements framework loose to allow sub-systems to establish their own requirements based on their specific external environment.

CSIS analysis of the case studies shows the enterprise model has produced favorable results in cases where it was applied. In several cases, executives from SoS acquisition organizations and program offices indicated that their attempts to be more focused on enterprise-wide governance have been challenged by the existence of specific acquisition standards created without a focus on the challenges unique to complexity. Thus, new policies and governance models are needed in order to facilitate more uniform application of the model and flexible use of best practices illustrated in each of the cases.

Counter Rocket, Artillery, and Mortar

The Counter Rocket, Artillery, and Mortar (C-RAM) system is an Army asset used to detect and destroy rocket, artillery, and mortar threats. The C-RAM acquisition effort was initiated through an operational need statement (ONS) issued in June 2004 and validated three months later in September of that year (Director of Operational Test and Evaluation, 2006, pp. 51–52; United States Army, 2010). Due to initial reliance on non-developmental items (NDI) and existing assets, the Army was able to field its first full C-RAM system by late 2005, only 15 months after the issuance of the ONS ("Army to Field," 2005).[6]

---

[6] The Army had started fielding the C-RAM in mid-year, with the deployment of the SENSE and WARN sensor systems.

Table 8. Counter Rocket, Artillery, and Mortar Governance Attributes

Governance Attributes	Program Characteristics
Level of organizational focus	• Governance at program-level was supplemented by capabilities-level focus in other relevant programs • Capability-wide executive leadership concentrated in program directorate office • Strong political support within the executive leadership in the Army
Integration of functional end-user needs	• Direct interface with end-users allows timely consideration of changes requested and/or developed by the end-user • PM has approved 25 Operational Needs Statements since C-RAM deployment
Decision-making authority	• A program directorate (PD C-RAM) leads decision-making for C-RAM components and system purchasing, engineering, and modifications as necessary • Program managers at the levels of Program Executive Office (PEO), Department of the Army, and OSD are less involved, but offer direction on needs and program implementation
Enforcement	• C-RAM did not have formal enforcement mechanisms, but relied on aggressive development schedules to encourage stakeholder performance
Workforce	• Dedicated contracting and procurement workforce
Incentive structure	• Centralized leadership appeals to common mission to incentivize performance
Knowledge ownership/ access to knowledge	• PM agreed to protect contractor data and supply "truth data" from the testing and evaluation range in order to facilitate knowledge sharing • Contractors required to submit data daily when on the range, at threat of removal from the range in the event of non-compliance
Risk assessment/risk management	• PM assess all systems and system modifications through modeling and desktop validation to ensure interoperability • Testing at each stage of sub-system acquisition verifies interoperability and implementation of ICD

Note. This table comes from CSIS analysis.

C-RAM uses a system of sensor command and control (C2) visualization to detect threats, display the source of an attack, and warn of potential impact. Those sensors relay a threat's track to the intercept system and pass the point of origin and impact data to supporting systems to aid in the response. This SoS approach to the problem created a more capable weapons system than the sum of the individual component parts.

The Army initiated the development of C-RAM in order to obtain a solution for combating unconventional attacks on fixed assets from temporary short-range positions termed "shooting and scooting" (Corbett, Beigh, & Thompson, 2012). Insurgents in Iraq used these indirect fire tactics with low trajectory rocket and mortar strikes to hit targets while minimizing exposure to counterattack.

The program directorate C-RAM (PD C-RAM) has overseen the C-RAM acquisition effort since the inception of the program. PD C-RAM was originally

housed in PEO Command, Control, Communications-Tactical (PEO C3T), reflecting the network focus of the office's charter (Walker, 2010). However, the office transitioned to PEO Missiles and Space in May 2011 as the Army began consolidating its air and missile defense C2 structure (Walker, 2011).

Table 9. Counter Rocket, Artillery, and Mortar Systems and Components

System	Components
C2	Forward Area Air Defense Command and Control (FAAD C2)
	Air and Missile Defense Workstation (AMDWS)
SENSE	Lightweight Counter Mortar Radars (LCMR)
	Firefinder Radars
	Ka- and Ku-Band Multi-Function Radio Frequency Systems (MFRFS)
INTERCEPT	Land-Based Phalanx Weapon System (LPWS)
	Accelerated Improved Intercept Initiative (AI3)
WARN	Wireless warn
	Wireless Local Area Network (LAN)

Note. This table comes from CSIS analysis.

Table 9 outlines C-RAM's component systems. These include an audio/visual emergency warning system and direct network access through a wireless local area network. In the event of an attack, C-RAM uses a direct link across Army, Marine, and Air Force command and security systems. This information sharing across forces and services allows for improved data analysis and more effective anticipation of indirect attacks. For example, using C-RAM attack trend data, analysts determined a significant decrease in indirect fire during Islamic Holy Days and an increase during Western and Christian holidays. Data sets such as these allow forces to project likely trends in the number of indirect attacks against forward fixed asset positions.

C-RAM leveraged existing technologies within the DoD and private sector to curtail the typical system-of-systems acquisition timeframe of 10–20 years. The project brought the concept from its to reality in just 15 months. C-RAM development followed the Joint Capabilities Integration Development System (JCIDS), which focuses on defining operational requirements and evaluating solutions from an operational perspective. Understanding the operational environment and clearly framing the problem contributed to developing an effective solution (Corbett et al., 2012, p. 50).

The program office has led several improvements to the C-RAM system-of-systems since its deployment. The Accelerated Improved Intercept Initiative (AI3) is one example that illustrates the program's ability to quickly respond to changing and emerging end-user needs. Program leaders began developing this missile interceptor sub-system in response to a need for intercept capabilities beyond those offered by Land-Based Phalanx Weapon System (LPWS). In order to develop and deploy this sub-system quickly, the program office used major components already

mature and fielded. This contributed to a quick acquisition period; the program office closed a competitive contract on AI3 in less than five months after its initial solicitation, and conducted successful live-fire tests just 18 months later. PD C-RAM led the development of the Ku Radio Frequency System (KRFS) fire control radar to complement the AI3 system.

It is difficult to quantify the amount of funding that has been directed to the C-RAM program. Funding has come from multiple budgets. The Army's procurement budget alone shows that C-RAM has received $1.5 billion of direct funding over its lifetime ("Counter-Rocket, Artillery & Mortar," 2011). The figure may be much higher if funding for operations and maintenance (O&M), operations at forward operating bases, and some of C-RAM's more advanced components, such as the SENSE and WARN sensor systems, are included.[7] OCO funding served to generate the initial system-of-systems, and cross-service O&M funds and Army Research, Development, Testing and Evaluation (RDT&E) outlays directed mostly at sensor development were critical at later stages to enable quick response to emerging needs.

Despite funding uncertainty, however, the Army has delivered C-RAM without clear evidence of cost overruns. In fact, cost-effectiveness appears to be one benefit of PD C-RAM's decision to use mostly NDI to fulfill the Army's urgent operational need. The program was also successful in delivering assets to end-users on schedule.

Distributed Common Ground System

Since 1998, the DoD has invested billions in the development of technologies to network ISR assets across services and ensure their interoperability.[8] The result of this investment is a family of intelligence systems known as the Distributed Common Ground System (DCGS). The DCGS case demonstrates the value of a sophisticated and agile workflow, as well as the value of open source standards for technology development.

---

[7] For an example of additional funding and contract activities dedicated to C-RAM, see the Defense Information Systems Agency's (2011) report, "Counter Rocket, Anti-Mortar Sense and Warn Forward Operating Base (FOB) Staffing and Operations."

[8] The DoD began investing in the DCGS concept in 1998, but the requirements for the program were not set until 2003. In that year, a joint working group received approval of its Capstone Requirements Document for the DCGS system from the Joint Chiefs of Staff. For more on the DCGS system's history prior to program approval, see Director of Operational Test and Evaluation (2002).

Table 10.   Distributed Common Ground System Governance Attributes

Governance Attributes	Program Characteristics
Level of organizational focus	• Program-level focus at each of the four service DCGS Program Manager offices • Standards, facilitate integration of systems developed at the program level within the enterprise
Integration of functional end-user needs	• Throughout the program, warfighter needs have driven development of assets and procurement of NDI
Decision-making authority	• Centralized at program manager level, with selected areas of oversight from PEO • PEO provides strong political cover for program manager decisions
Enforcement	• No funding for integration, and no mechanism to force integration
Workforce	• Dedicated, long-term leadership facilitates expertise and commitment to mission • Support staff promoted from within
Incentive structure	• Few fiscal incentives exist to encourage cooperation with DCGS program goals • Barriers to entry into the DCGS SoS architecture are low
Knowledge ownership/ access to knowledge	• Core software architecture adjusted to an open-source standard only upon pressure by DCGS customer stakeholders; allows easy collaboration and information sharing among developers • Standards prevent substantial stovepiping and allow independently developed components and sub-systems to interoperate
Risk assessment/risk management	• No evidence of substantial risk management tools or metrics for assessment

Note. This table comes from CSIS analysis.

Prior to the rollout of DCGS, intelligence analysis was largely de-centralized. There was little discussion of intelligence or its sources across the services. Collaboration on gathering, processing, and dissemination of data was also lacking. The DCGS effort originated as an attempt to facilitate data-level interoperability through the use of common software architecture, the DCGS Integrated Backbone (DIB).

DCGS planning segregates contracting, development, and procurement activities among the services. Each of the four armed services components acquires network assets specific to its own needs. The individual networks operate on the DIB, a software system incubated within the Air Force DCGS (AF DCGS) program and later expanded to all of the service-specific networks in April 2005 ("Navy Looks Forward," 2005).

The Army DCGS (DCGS-A) operates as a field tactical data cloud for Afghanistan, which incorporates rapid updates of information with real-time communication. This allows analysts to perform better data analysis and adapt to changing support needs. Leveraging cloud storage and processing allows for more a more agile response and better analysis in the field. The Army is working to field a browser-based interface through smart phones and tablets to allow for better access to the system.

No single organization or office holds responsibility for ensuring the service-specific DCGS systems are interoperable. Instead, enterprise-wide deployment of DIB as a common foundation for the DCGS family of systems ensures integration and interoperability. The DIB Management Office (DMO) has provided oversight for that effort under the direction of an Air Force program lead. Aside from this mechanism, each of the four services has substantial autonomy in acquiring its own DCGS system.

Despite its lack of an overt, top-down governance structure, the DCGS acquisition effort has progressed on-schedule and without major cost overruns. However, this has not shielded the acquisition effort from criticism altogether. Service intelligence officials and congressional oversight sources complain that the DCGS effort creates wasteful acquisition redundancies across the services, restricts access to low-cost commercial IT alternatives and results in asset obsolescence at time of fielding ("U.S. Air Force Joins Navy," 2009; "Four House Lawmakers," 2013). CSIS analysis also suggests the DCGS bottom-up governance approach makes it difficult to determine the level of investment in the system and the performance of individual asset acquisition efforts.

Global Nuclear Detection System

The Global Nuclear Detection System (GNDS) is an informal acquisition effort with the backing of USD(AT&L). It consists of fragmentary acquisition programs from the DoD, Department of Homeland Security (DHS), and non-proliferation agencies nominally connected by a shared goal.

Table 11.   Global Nuclear Detection System Governance Attributes

Governance Attributes	Program Characteristics
Level of organizational focus	• Program-level focus guided by an overarching, enterprise-level policy directive
Integration of functional end-user needs	• Current system of lax governance, combined with absence of GNDS-specific acquisition programs, has suppressed the degree to which the system meets end-user needs
Decision-making authority	• Decision-making authority does not go beyond the level of program managers for GNDS-relevant technologies
Enforcement	• No enforcement mechanisms are in place to ensure compliance with GNDS objectives
Workforce	• GNDS itself has no dedicated workforce due to the fragmentation of programs across different departments and agencies
Incentive structure	• Decision-making authority does not go beyond the level of program managers for GNDS-relevant technologies
Knowledge ownership/ access to knowledge	• GNDS program managers indicate in interviews with CSIS that knowledge sharing has been difficult in the program because without an overarching purview, visions on the GNDS differ among the various stakeholders • There were also related issues with communication, in which it has been difficult to coordinate and synchronize the vision and mission across the numerous relevant entities
Risk assessment/risk management	• No measures have been taken to assess or control for risk at the moment, reflecting the immaturity of the effort

Note. This table comes from CSIS analysis.

The detection of nuclear and radioactive threats is a broad undertaking that encompasses activities within both the civil and defense realms. For this reason, the DoD has taken the position that a single technology or family of technologies alone cannot meet the challenges of nuclear detection, especially on a global scale. As a result of this position, GNDS has not codified into a formal system-of-systems or program. Instead, the DoD has mostly looked at nuclear detection through the lens of interagency coordination. Several offices within the DoD have contributed, with particular leadership from the Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs within the OUSD(AT&L).

Due to its informal nature, and because authorities have not allocated funding for GNDS, it is unclear how successful this effort has been. Research uncovers no evidence that individual agencies have undertaken acquisition with the explicit purpose of achieving the GNDS goals outlined by the USD(AT&L) Treaty Compliance and Homeland Defense Coordinator. Furthermore, although policies exist on countering weapons of mass destruction (WMD) and nuclear threats, no guidance has been offered in what GNDS requirements are, how a completed GNDS solution would be structured, or timelines for GNDS capabilities roll-out.

The Global Nuclear Detection Architecture (GNDA) exists as a model of what GNDS might look like if it is to become a program of record. In the absence of meaningful acquisition activity under the GNDS family, the DoD mostly has ceded

the lead role in global nuclear detection to the Domestic Nuclear Detection Office (DNDO) in DHS. DNDO leads GNDA as a federal-civilian, cross-agency system-of-systems responsible for detecting nuclear and radiological threats in the homeland. A network of radiation detection equipment comprises the backbone of GNDA, with much of the program's outlays directed toward the procurement and maintenance of these assets. In contrast with this approach, the DoD's nuclear detection efforts are less coordinated. Individual offices pursue nuclear detection technologies consistent with GNDS goals, but there is no governance mechanism in place to ensure the interoperability of those systems, nor to enforce acquisition best practices within sub-systems.

While GNDA provides one example of how GNDS could be governed if it were to become a formal PoR, challenges in its implementation also illustrate areas where complexity complicates the acquisition of the system-of-systems. As with GNDS, the GNDA model has been criticized for loose program requirements and a lack of cross-agency coordination (Biesecker, 2008). To the extent that the DoD begins pursuing GNDS more aggressively without a clearer definition of the system-of-systems' objectives and end-state, it is likely to encounter challenges resulting from the varied level of commitment to the GNDS mission from stakeholder organizations.

Harvest HAWK

The Harvest Hercules Airborne Weapons Kit program—Harvest HAWK, for short—is the Naval Air Systems Command (NAVAIR) effort to equip KC-130J Hercules refueling tankers with a weapons kit and ISR capabilities. The project met the need for an armed KC-130J variant for Close Air Support that the USMC outlined in its universal need statement on July 21, 2008 ("DoD Finalizes C-130," 2008). Naval Air Systems Command, the contracting agency for the program, oversaw a development process that brought the HAWK to theater in less than two years, from the need statement in July 2008 to Initial Operating Capability (IOC) on October 13, 2010 ("U.S. Naval Aviation and Weapons Development in Review," 2012).

Table 12. Harvest HAWK Governance Attributes

Governance Attributes	Program Characteristics
Level of organizational focus	• Operational needs statement dated July 21, 2008 outlined the need for an armed KC-130J for close air support.
Integration of functional end-user needs	• Modifications of the system in development have directly incorporated end-user needs. Examples include the derringer door modification, which allows crews to discharge munitions without depressurizing the main cabin.
Decision-making authority	• Flat leadership structure with clearly designated decision-making authority
Enforcement	• No enforcement mechanisms observed
Workforce	• Small, agile workforce with technical expertise and high familiarity with operational needs
Incentive structure	• Because Harvest HAWK was not competed but instead given to the C-130 airframe supplier, strong incentives were not in place to ensure timely and cost-effective delivery
Knowledge ownership/ access to knowledge	• Flat, lean structure of program team prevented the emergence of significant obstacles knowledge access
Risk assessment/risk management	• No risk management mechanisms observed • The Marine Corps mitigated most risks upfront by using highly mature and commercially available products

Note. This table comes from CSIS analysis.

The DoD carried out HAWK contracting in a piece-meal fashion, with one round of kit development followed by several rounds of unit purchase and aircraft modification contracts. Lockheed Martin won a $22.8 million sole-source contract for the development of HAWK in May 2009 ("Fuel and Fires," 2009). Under the terms of the contract, NavAir agreed to purchase one development HAWK. The contracting office later awarded Lockheed Martin a $21.3 million contract in September 2009 for the purchase of two additional units (Department of Defense Information, 2009). As of this writing, total purchases include six D-Kits (roll-on/roll-off mission kits) and 10 KC-130Js carry the HAWK (United States Marine Corps Center for Lessons Learned, 2012).

HAWK consists of a Lockheed Martin AN/AAQ-30 Target Sight System (TSS), as well as AGM-114 Hellfire missiles and a 30mm cannon ("Marines to Deploy," 2010). Some kits also carried a ramp-mounted release system for "Gunslinger" precision-guided munitions (United States Naval Institute, 2012). The Marine Corps installed a "derringer door" modification in 2012 to allow the HAWK-equipped KC-130J aircraft to fire MBDA GBU-44/E Viper Strike glide munitions while the aircraft remains pressurized, reducing the time and preparation necessary for weapons deployment ("Harvest Hawk Tests Prove Successful," 2012). Of the kit's components, only the TSS—which entered IOC in April 2009 as a component of the AH-1Z Cobra aircraft—was in development at the time of the initial contract in April 2009 ("Lockheed Martin Delivers First Target," 2009).
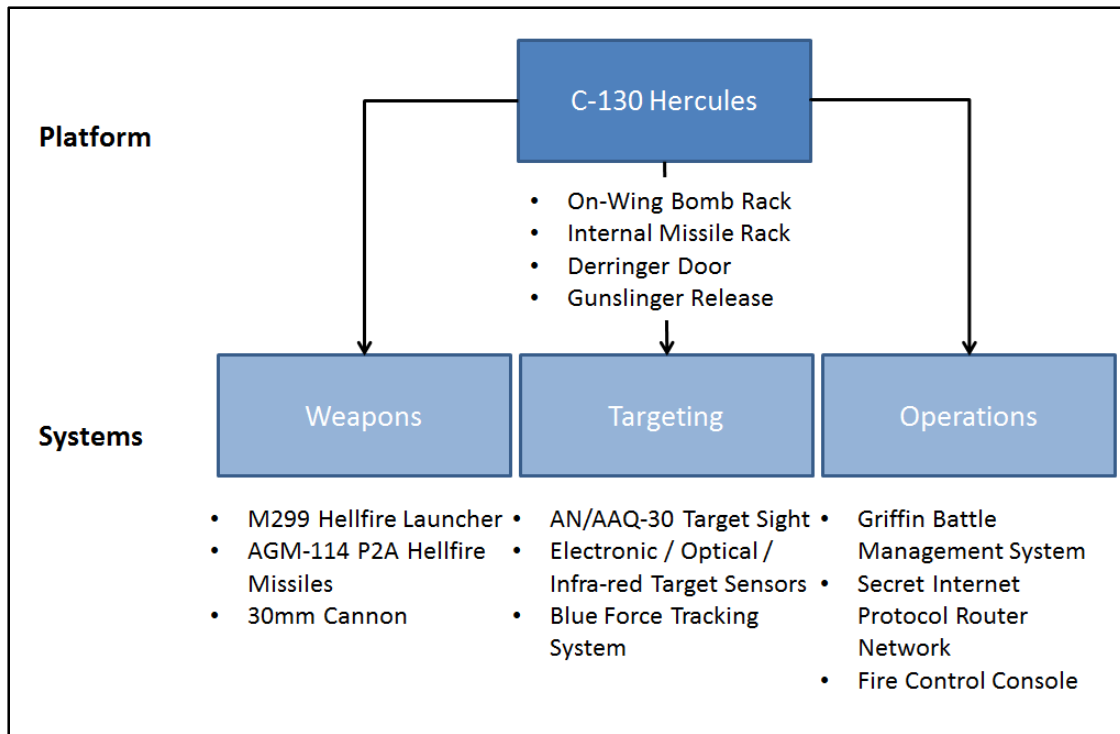
Figure 3.   Harvest Hercules Airborne Weapons Kit System Components

The Harvest HAWK system adds a lethal edge to a long-standing Marine Corps air platform. Harvest Hawk crews provide close air support to ground forces and can sustain this air support longer than conventional fighter jets or helicopters. The system has been vital to ground troop support in remote regions such as the Helmand province in Southern Afghanistan.

Combined with a contracting process that allowed for the purchase of HAWK units in successive procurement rounds, the contracting office's decision to use NDI to meet the Marines Corps urgent need request contributed to the success of the Harvest HAWK acquisition effort. Apart from some delay in incorporating the 30mm cannon into the roll-on/roll-off kit ("Official," 2011), the program managers achieved success without cost or schedule overruns. Acquisition officials also were able to address substantial drawbacks of the ramp-mounted munitions release system—that it required operators to depressurize before releasing Gunslinger munitions and to remove the apparatus to allow the KC-130J to perform cargo transport missions— with the installation of the derringer door (Roosevelt, 2012). Thus, when viewed in isolation, the Harvest HAWK program stands as a model for successful SoS acquisition through a contracted LSI.

Harvest HAWK also serves as a useful case for demonstrating the importance of continually integrating end user needs into the system and its components. The developers used an existing and widely accepted platform, the C-

130, with kit-based components and other modifications to meet the warfighter's needs in the field. The installation of the derringer door to reduce the deployment timeframe for the system represents an improvement directly based on end-user feedback.

Maritime Domain Awareness

Maritime Domain Awareness (MDA) is an international, interagency strategy to deal with threats and challenges in maritime theaters. When it is completed, the MDA system-of-systems will be able collect, fuse, analyze, and disseminate data among defense, law enforcement, and border protection officials from the United States and allied countries to create a cross-domain common operating view. Analysis of the process of putting together MDA suggests the program illustrates that formal mechanisms are necessary in complex acquisition efforts to encourage commitment to the effort's mission among stakeholder entities, and the active involvement of those entities in the development and procurement of component systems.

Table 13.   Maritime Domain Awareness Governance Attributes

Governance Attributes	Program Characteristics
Level of organizational focus	• Implementation at sub-program level • Enterprise-level integration has been prescribed but not implemented
Integration of functional end-user needs	• MDA infrastructure integrates end-user needs as they were describe at program outset, but does not possess mechanisms for integrating new and changing needs • Sub-program funding allows for reverse integration, in which spiral technologies are folded into new needs
Decision-making authority	• Capabilities and funding decisions isolated at program level, where program executives choose whether and to what extent MDA should be incorporated in investment objectives
Enforcement	• No substantial enforcement guiding MDA-relevant programs to desired end state
Workforce	• No investments in new workforce development, relying instead on existing acquisition workforce at individual program offices
Incentive structure	• Program managers have no incentive to incorporate MDA objectives into requirements or acquisition operations
Knowledge ownership/ access to knowledge	• Informal knowledge sharing occurs through white papers and other forms of thought-leadership
Risk assessment/risk management	• Lack of meaningful leadership mechanisms creates high-risk environment with no identified tools for management of unforeseen circumstances

Note. This table comes from CSIS analysis.

The MDA concept originated from a 1998 presidential initiative and was developed further in National Security Presidential Directive 41 (NSPD-41) and Homeland Security Presidential Directive 13 (HSPD-13), both released on December 21, 2004. Since then, the technology investment strategy and the supporting offices and

business systems established to execute MDA have undergone numerous changes. Currently, the National Maritime Intelligence-Integration Office (NMIO), under the direction of appointees from the Navy and Coast Guard, is the nominal lead for MDA's information exchange portal, the open architecture tool at the heart of the MDA mission.

MDA does not necessarily consist of prescribed technologies. A number of policy directives have offered strategic direction on capabilities required; however, the participating agencies—primarily the USCG and Navy, with some additional contributions from Customs and Border Protection—have mostly led their own system acquisition initiatives. Most notably, the Navy planned two stages, or "spirals," of technology acquisition to develop and integrate the infrastructure MDA would need in order to enable maritime security capabilities. Table 14 outlines the specific technologies sought in the first spiral.

Table 14. Spiral 1 MDA Technologies

Technology	Acquisition Efforts
Electronic Maritime Interdiction Operations (E-MIO) Wireless	• Trident Warrior Exercises • Small-scale initial deployment on USS Cole
Comprehensive Maritime Awareness (CMA)	• Joint development with Republic of Singapore • Tool-kit development and technology refresh
Global Trader	• Office of Naval Intelligence (ONI) led development of Global Trader database and search engine
Google Apps & Earth	• Used in support of pilot programs for MDA, such as InRelief, a humanitarian database
MDA Data Sharing Community of Interest	• Coordination with stakeholder organizations • Testing of existing solutions
Maritime Global Network (MAGNet)	• Navy oversight for testing and integration • Coast Guard solutions analysis and development
Tripwire	• IBU led development of threat detection toolkits and deployed to targeted stakeholders
Law Enforcement Information Exchange (LInX)	• Development through Naval Criminal Investigation Service (NCIS)
FAST2CAP	• Deployment among U.S. and international defense and federal-civil stakeholders

Note. This table comes from CSIS analysis.

The Navy's process of selecting and developing technology solutions represents a departure from more traditional acquisition workflows. Similar to other acquisitions, the Navy released an Initial Capabilities Document (ICD) for "Data Fusion and Analysis Functions of Navy Maritime Domain Awareness" and identified shortfalls in cross-agency MDA capabilities in 2009. However, interviews with DoD officials indicate that the ICD reflects the Navy's position alone and does not necessarily correspond with specific requirements for other agencies (GAO, 2011). The Navy created and refined requirements for the technologies comprising the MDA system-of-systems through an iterative development process.

Through its iterative spiral approach to technology development, the Navy began with enterprise-wide requirements defining the doctrine, materiel, leadership and education, personnel, and facilities (DOTMLPF) necessary for the MDA mission. This first round of requirements identifies tasks each system or system-of-systems needs to accomplish. The Navy then selects a solution or a number of solutions to accomplish those tasks and tests them against specific objectives and metrics. The Navy then refines the requirements based on this testing and selects those solutions that best meet them. It then conducts another round of testing on those solutions. This process continues until the Navy reaches an end-state of DOTMLPF requirements and selects the most appropriate technology.

The E-MIO Wireless presents one example of this process as it operates in practice. The Navy tested E-MIO as a partial solution in 2006. At the time, the wireless network successfully completed a number of tasks involved in the interdiction of vessels. The Navy installed the kit on the USS *Cole* in April 2007. It also tested the kit in the 2006 and 2007 Trident Warrior exercises. Lessons learned from these initial operations and tests contributed to refined requirements, lessons learned analysis, and a refresh of fielded iterations (Ackerman, 2007).

Analysis of budget requests from 2009 to present day show that, to date, services have procured MDA assets mostly under the umbrella of larger program elements. For example, in the case of the E-MIO Wireless network kit described here, the PEO for Command, Control, Communications, Computers, and Intelligence (C4I) led the development of that technology without any formal or statutory coordination amongst other MDA stakeholders. Furthermore, with the exception of some Office of Naval Research (ONR)-led research and development (R&D) programs, the services have procured primarily NDI and commercial off-the shelf (COTS) products. As a result of this approach to acquisition, investments in MDA are difficult to quantify, progress is difficult to monitor, and oversight is difficult to ensure.

Results of Interviews

The case summaries above offer descriptive, program-specific attributes related to the governance of complex SoS acquisition efforts. In addition to the attribute-specific information presented here, interviews with acquisition executives suggest that an agile and multi-layered governance process can lessen the operational burden of managing and delivering complex systems-of-systems. Furthermore, strong enforcement mechanisms are necessary to ensure outcomes are in line with expectations.

In order to capture specific best practices from the perspectives of those involved in specific example programs, the CSIS research team conducted

interviews based on its established framework of eight governance attributes. Researchers conducted 11 interviews in total with the participation of 17 acquisition executives. Each interview lasted about 1–2 hours and was semi-structured to allow interviewees to stray from the explicit governance attributes and provide more general commentary on acquisition challenges. Each program has at least one interview associated with it in order to ensure broad coverage of all case studies.

Following each interview, researchers compiled key points according to attributes and periodically categorized them into broader findings. Interviewers loosely structured the interview sessions around the role of each attribute in the specific case. Collectively, information gathered from interviews serves to aggregate and organize expertise on the subject of acquisition governance for analysis of best practices.

Collectively, the conversations suggested that five themes are critical to understanding governance of complex acquisition. These themes are presented here in order of importance to governance.

Theme #1: Stakeholders must maintain focus on the end-result of an acquisition effort at the enterprise level.

First, complex acquisition governance requires that all stakeholders maintain focus on the end-result at the enterprise level. This structural issue is central to a system's ability to operate in an environment consisting of multiple other systems. Interviewees suggest that a narrow focus—focus on a specific product or capability set, for example—compromises the value of a single system's acquisition to the overall objectives of the system-of-systems and its user communities. This narrow focus also contributes to demand uncertainty in instances where stakeholders simultaneously develop multiple competing capabilities to accomplish the same end goal.

FCS offers several insights about the impact of a product- or program-level focus on the success of an acquisition effort. A former DoD acquisition official involved in overseeing FCS reports that many in the acquisition community charged with approving the program at its various 5000-series milestones were frustrated that its network components duplicated the functions of existing technologies. Furthermore, the source continues, FCS had no roadmap for integration with interacting systems, namely the Warfighter Information Network-Tactical (WIN-T), an all-encompassing Army tactical network program, and Joint Network Node (JNN), a SatCom system. One interviewee criticized the program for attempting to build its own operating systems, called SOSCO, from scratch rather than use existing operating systems able to interface with WIN-T and JNN. The engineers had no plan for bringing those pieces together, and testing their interactions required that the entire system first be fielded, the interviewee reports.

Interviews with several program executives and stakeholders provide an important nuance to the importance of enterprise-level focus. In cases such as FCS where focus is narrow, problems emerge where the feasibility of end-state integration is unclear. Integration problems also surface in cases where enterprise-focus is present, however. In MDA, for example, acquisition executives maintained a focus on the objectives of the entire enterprise, but were presented with challenges to enterprise-wide integration all the same.

Theme #2: A layered decision-making structure with distinct, delegated authority must be clearly established at the outset of complex acquisition efforts.

The reason for integration problems, even in those programs in which organizational focus is held at the enterprise level, underscores a second theme about complex acquisition governance. It suggests that a layered decision-making structure with distinct, delegated authority must be clearly established at the outset of complex acquisition efforts in order for their level of organizational focus to matter.

Interview results show that the various process constraints faced by each of the acquisition case studies—for example, clarity and consistency of scope, availability of personnel, inventory of resources, and so forth—are attributable in part to their decision-making structures. Process constraints also translate to poor outcomes in cases where decision-making structures were not designed to meet the specific needs of an acquisition effort, or where decision-making authority was weak or non-existent.

The MDA effort demonstrates the challenges created by weak and heavily centralized decision-making authority. In that case, interviewees report that the Executive Agent for MDA (EAMDA) has notional leadership over stakeholder agencies, but no real decision-making authority. Instead, it serves in the role of what one interviewee calls a "broker and a cheerleader." Formally, EAMDA issued an Initial Capabilities Document (ICD) to allow material solutions development under the standard defense acquisition process. However, there is no formal lead for requirements generation or subsequent acquisition decisions. As a result, stakeholder agencies have different perceptions of the MDA charter and what technologies satisfy its core mission objectives. These definitional issues emerge in the absence of strong central leadership. Interviewees support this observation and report similar challenges in the GNDS case study.

The DCGS case contrasts with the MDA case because the DCGS decision-making structure is relatively well-suited to the mission objectives of that acquisition, particularly in its decentralization. One DCGS executive reports that DCGS decision-making is conceptually separated into recommendation and implementation functions. This concept is mapped in Figure 4, which outlines the DCGS

organizational structure and the processes involved in key functions of an acquisition.
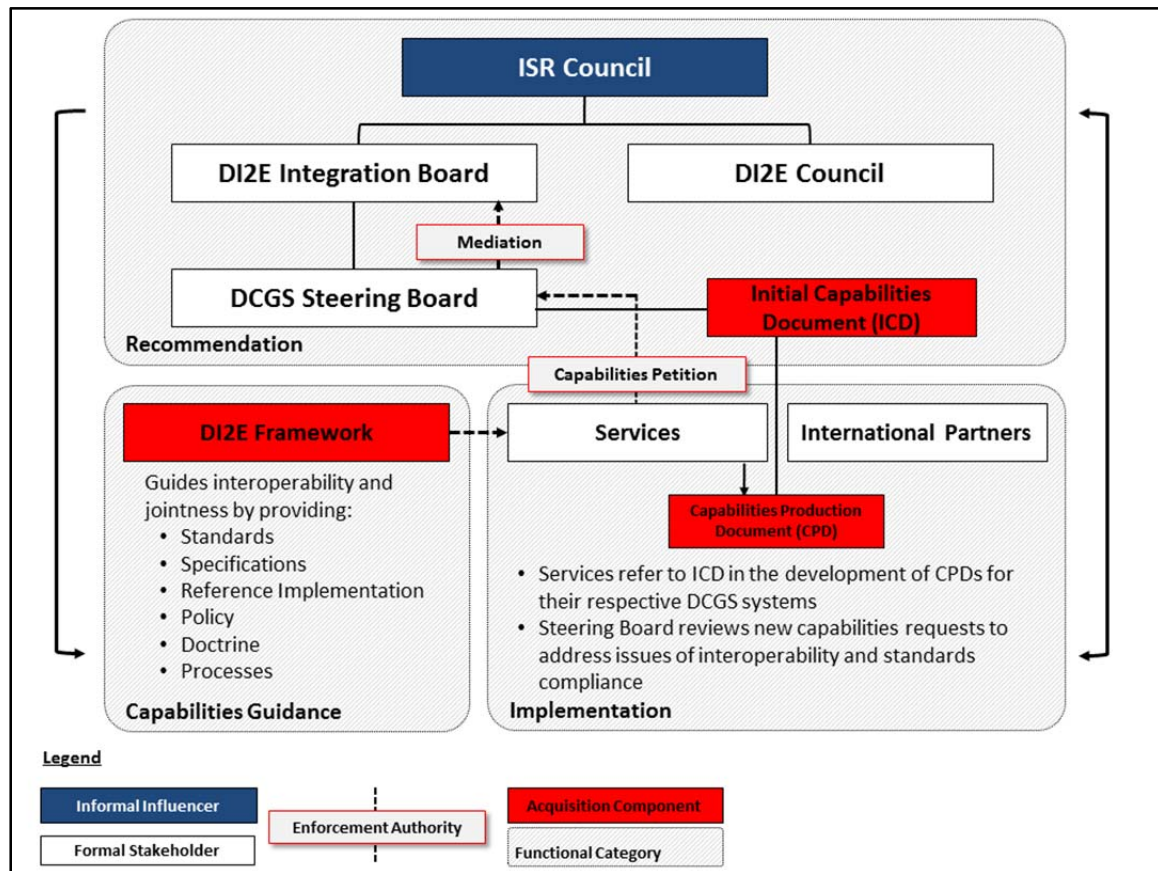

Figure 4.   Distributed Common Ground System Conceptual Governance Structure and Key Acquisition Processes

The DCGS Steering Board serves as a strong, central leadership entity to provide capabilities guidance and keep development and procurement efforts aligned with core mission requirements. The Army, Air Force, Navy, and Marine Corps each have their own lead entities for the implementation functions. Each of the service components refers to the ICD to draft Capabilities Production Documents (CPDs) for each of their respective systems. The DCGS Steering Board then reviews the new capabilities to determine their fit with the standards and specifications established in the ICD and governed by a central interoperability framework, the Defense Intelligence Information Enterprise (DI2E). Similar to MDA and GNDS, this workflow represents an agile approach to decision-making that empowers end-user communities with substantially different requirements to make their own procurement decisions. However, it is supplemented by strong, formalized central leadership.

Theme #3: Decision-makers must design effective management and enforcement mechanisms and integrate them into the acquisition process.

Interviewees suggest that enforcement mechanisms are the critical component tying together the enterprise focus with product-level decision-making. In order to maintain short chains of authority between the technical communities at the bottom of the production chain with the enterprise-level planners at the top, decision-makers must design effective management and enforcement mechanisms and integrate them into the acquisition process. Formalized program management mechanisms consisting of a well-defined set of performance criteria have the advantage of lessening the process burden of complex acquisition. With complementary incentives and metrics for monitoring performance, enhanced program management can also contribute to improved cost and schedule outcomes.

The process advantages of effective program management are apparent in the DCGS case. The DCGS effort runs an overarching recommendations and review process through the DCGS Steering Board, but delegates acquisition implementation to individual end-user communities based on a common set of standards established in the DI2E Framework. At the systems level, the acquiring service can approach risk in technology acquisition on a case-by-case basis. The acquiring armed forces component can also design its contract or contracts based on the scale of a particular acquisition item, or whether the acquisition is developmental or non-developmental. At the enterprise level, the DCGS Steering Board has a mediation process through which it can deny efforts that it determines to be too risky or that do not contribute to the DCGS mission objectives.

The effectiveness of the DCGS program management structure is particularly apparent when compared with the management systems used in other large complex acquisition cases, such as Future Combat Systems (FCS) and Integrated Deepwater System (Deepwater). In these cases, acquisition was directed through single, service-centric programs-of-record. An overarching rule-set was applied to all subordinate efforts. Sources interviewed suggest DCGS has avoided the process rigidity that plagued FCS and Deepwater in part because of its separation of top-down program recommendations and bottom-up program implementation.

Theme #4: Program leadership must prevent vested interests and cost concerns from becoming barriers to knowledge ownership.

Organizational focus at the enterprise level, driven by clearly delegated decision-making authority, and supported by effective enforcement mechanisms, creates the underpinnings of a complex governance structure. However, any one of these components can be compromised when stakeholders are unable or unwilling to share information. This points at a fourth theme in complex acquisition governance: In order to execute a complex acquisition effort effectively and

efficiently, agencies and offices partnered in the technical development of systems as well as the duties of program management must be able to access and share information among themselves. Oftentimes, barriers to knowledge access can inhibit the success of a complex project. Conversations with interviewees suggest that knowledge access also depends on strong incentives for active sharing of information about technologies, program goals, and progress toward established milestones.

Interviewees indicate that there are two types of barriers to effective information sharing and knowledge access. The first barrier is knowledge protectionism. Especially in instances of collaboration between private sector stakeholders, conversations with interviewees suggest that companies are more likely to withhold information from partner entities due to competition for other government contracts. This concern was especially strong in early efforts to make the DCGS Integration Backbone (DIB) software package open-source. In an effort to facilitate software revisions to more effectively meet the needs of individual end-user communities, the DCGS Steering Board and DI2E Integration Council were strongly supportive of revealing the DIB source code to the development community. However, according to one program source, the DIB parent developer resisted efforts to make the software open-source. In the end, DCGS customer offices were able to compel the contractor to share its knowledge.

Program challenges resulted from early resistance to revealing the DIB software code. By compelling its primary software contractor to open its code for other users to access and develop, the DCGS program office demonstrated how a large organization can hedge against knowledge protectionism. Using the code, DIB challenger MarkLogic successfully developed a version of the DIB based on Extensible Markup Language (XML, an open-standards software encoding format) to more adequately meet the needs of a sub-segment of the broader end-user community. Namely, MarkLogic's DIB was a better fit for United States Special Operations Command (USSOCOM or SOCOM), which had a need for a high-performance reconnected-ops DI2E.

A second barrier to information sharing is created by differing levels of information management capabilities. Levels of technical astuteness can be widely different between government customers and industry suppliers. This problem is compounded by varied clearance privileges required for access to, and use of, compartmentalized information. Sources interviewed indicate this problem has complicated several systems-of-systems acquisitions. Interviewees suggest that information needs among stakeholders in MDA are challenged both by the breadth of information collected and the need to filter it to lower levels of clearance, especially unclassified civil users in the Coast Guard. For participants in the

Hercules Airborne Weapons Kit effort—known more commonly as Harvest HAWK—data relevant to that program were only accessible through a single computer network, requiring physical ownership of the data for effective information sharing. Sources point to these barriers as real and addressable challenges to acquiring and integrating systems-of-systems.

Theme #5: Leaders at each level of the system-of-systems must be adaptable to changes that result from human behavior.

A fifth and final theme of complex governance reported by interviewees observes that leaders at each level of the system-of-systems must be adaptable to changes resulting from human behavior. This theme is applicable not just to the acquisition of complex systems-of-systems involving many components and stakeholders, but also to other systems in the natural world. Human behavior is the ultimate uncertainty, and agility is critical to absorbing the impact of its changes.

Within SoS acquisition efforts specifically, effective governance will recognize changes in the needs of a system's end-users early and reevaluate the usefulness of a planned acquisition. This feedback loop can be formalized through component-level proposals for new capabilities (MDA). It can also be more *ad hoc*, incorporating standards-based innovations developed by end-users into the completed system-of-systems (DCGS). In either case, the DoD 5000 series approach to acquisition appears to limit responsiveness to end-user needs.

In general, effectiveness appears to share a strong correlation with cases that were initiated with a clear end-user in mind. For example, the Harvest HAWK acquisition was born out of the necessity to provide air support for Marines in Afghanistan. The Marines were deployed to train Afghan security forces. Although they were not under the purview of Marine Air-Ground Task Force (MAGTF), they developed an urgent need for air support when their training unit encountered persistent attacks from adversary forces. Information obtained from the Marines provided an impetus for the Harvest HAWK acquisition effort, making this case particularly representative of the effective use of human information inputs to produce and procure capabilities specifically answering the needs of the end-user.

An additional aspect of human input is the workforce that a system-of-systems effort has at its disposal. A good technical and program management workforce can make the difference between an effort's success and failure. Recruiting a truly great workforce can dramatically improve both the magnitude of a system's success as well as the process required to develop and procure it. Here, interviews suggest Harvest HAWK provides an example of the importance of skilled technical personnel supplemented by experienced program managers. A former program source indicates that Harvest HAWK's success in delivering a complex capability in a small period of time is attributable in part to the ability of the program

management to take advantage of the technical workforce available through NAVAIR.

Several other cases illustrate that a strong program management workforce is not as effective in delivering a system-of-systems capability when it has a weak technical workforce at its disposal. Sources suggested that workforce strength is not measured by technical skillsets alone. Rather, complex acquisition efforts benefit when their workforce is empowered to use its technical know-how to innovate new approaches to problems.

Although technical astuteness tends to reside with human capital in engineering functions, program managers often mistake general capabilities needs with prescriptive technical requirements under the existing framework for acquisition. Sources interviewed suggest that there is structural resistance to bottom-up innovation of new approaches to meeting capabilities demands. For example, one interviewee from the Harvest HAWK program indicated that a problem with coding on the Harvest HAWK's gimbal kept a team from the program office and the lead contractor in a room collaborating for weeks to find a fix. In the end, an engineer from the program team was separated from the effort and replaced with a new engineer. The new engineer recognized the flaw in the code within an hour, rescuing the program from further delay. The engineer was able to accomplish this in part because he was empowered to contribute his unique knowledge of coding.

A New Model of Systems-of-Systems Acquisitions

By combining the outcome and process challenges observed in the case studies above with in-depth, original data aggregated through interviews, CSIS developed the acquisition model presented in Table 15.

Table 15.   Best Practices in Systems-of-Systems Acquisition

Governance Attributes	Program Characteristics
Level of organizational focus	• Program-level focus supplemented by overarching enterprise-level governance and short authority chains
Integration of functional end-user needs	• Kit-based, modular systems allow timely integration of end-user needs and changes in the external environment • End-users are encouraged and empowered to develop their own sub-systems solutions in compliance with established SoS standards
Decision-making authority	• Stakeholders are given relative autonomy to make systems-level decisions based on standards and common operating environments installed at the enterprise-level • A central governance oversight body holds auditing and enforcement powers in order to maintain commitment to a system-of-systems' core objectives
Enforcement	• Enterprise-level authorities maintain ability to review and revise gate decisions as sub-systems evolve and needs change • Clear, systems-specific reporting requirements are established based on technological maturity and projected development schedules to support enforcement authority
Workforce	• Systems-level technical workforce includes recent or one-time end-users in order to create greater symmetry between end capability and changing user needs • SoS-level technical workforce is small and agile to avoid parochial interests • Lean but dedicated programmatic workforce to create and support technical expertise
Incentive structure	• Uses budgetary and personnel levers to foster mission commitment and compliance with established standards • Low barriers to the entry of new technologies and the innovation of existing solutions
Knowledge ownership/ access to knowledge	• Leadership shows sensitivity to the wide range of information-handling capacity and ability of different stakeholders throughout an organization to manage and understand information • Leadership also campaigns to accommodate those stakeholder entities with lower information-handling capacity and ensure their interests are also incorporated into the information feedback loop • Standards and network backbones are freely shared amongst stakeholders to encourage user-level innovation and collaboration
Risk assessment/risk management	• Critical technologies are highly mature and COTS where possible • Clear, measurable metrics are established to monitor less mature technologies and changes in the external environment

Note. This table comes from CSIS analysis.

Analysis of Best Practices

The analysis extracted these best practices based on a force ranking of the impact of performance in any single attribute on the process and outcome of each individual case study. CSIS independently assessed success factors in the attributes and supplemented analysis with primary input from sources interviewed. This approach facilitated analysis by incorporating the existing literature on complex systems with the expertise of acquisition executives with intimate knowledge of an individual case or multiple cases.

Critical Best Practices

An assessment of the case studies shows that success in three attributes in particular is critical to SoS acquisition. Those attributes are level of organizational focus, decision-making authority, and enforcement. The attributes are closely related and strong performance in any one is dependent upon performance in the other two.

Organizational focus at the enterprise level is critical to enabling SoS integration and facilitating flexibility for quick and substantive response to changes in the external environment. Although critical, enterprise-level focus is limited when it is not supplemented with some program-level focus on individual capabilities. The DCGS case, for example, shows the value of allowing programs and sub-system acquisition efforts to govern themselves to a certain point.

The key to differentiating these two levels of focus and ensuring that they interact with and respond to one another is in part related to the decision-making authority attribute. At the program level, stakeholders should be delegated the authority to make decisions about systems and technologies with a low burden of approval from the enterprise-level. This is especially important in complex systems-of-systems. The organizational legwork a program has to perform in order to approve a new sub-system that has newly developed or emerged as an end-user need can prevent the program from timely and effective integration of that technology or capability.

One way to achieve the right level of agility in decision-making delegation is to establish open-source standards for new technologies and systems as a replacement for traditional, formal oversight mechanisms. In interviews with CSIS, several Coast Guard executives indicated that it is already implementing this best practice post-Deepwater to ensure interoperability among C4ISR systems across its fleet of surface vessels and aircraft. Interviews also indicate DCGS revealed its DCGS Integration Backbone (DIB) for open source use, allowing industry to create a new and specialized XML-based search engine in order to meet a very specific end-user need. Therefore, this best practice assists decision-makers at the enterprise level by lessening their programmatic requirements, and empowers decision-makers

at the program level, as well as end-users themselves, to reflect SoS ecosystem changes in their planned acquisition activities.

The enforcement attribute links decision-making authority with level of organizational focus. Effective enforcement mechanisms enable enterprise governance authorities to keep program managers on-cost and on-schedule while easing the operational burdens associated with delivering large, complex systems-of-systems. Although statutory mechanisms for enforcement are established in the DoD's standard acquisition process, case study analysis finds those mechanisms custom-tailored to the specific demands of the individual system-of-systems to be most successful. For example, the DCGS effort created a central authority to review petitions for capabilities from an enterprise perspective, and reserves the right to deny an sub-system acquisition effort in the event that it is determined to be incompatible with the SoS objectives. This exists outside of the standard DoD acquisition enforcement mechanisms. Furthermore, the case of Future Combat Systems (FCS) illustrates how existing mechanisms can in fact be counterproductive and conceal underlying problems in a complex SoS acquisition effort.

Enabling Best Practices

In addition to the critical best practices, performance in the remaining attributes enables SoS acquisition efforts to reach end capabilities with fewer cost and schedule problems. These enabling best practices also contribute to greater alignment between a system-of-systems and the needs of its end-users. Finally, best practices in the remaining attributes help to mitigate problems of technology obsolescence and help ease the tendency for innovation in modern defense platforms to lag behind commercial industry.

Successful SoS acquisition efforts accomplish greater integration of functional end-user needs in part through the encouragement of innovation at the sub-systems level. One best practice in this regard involves the establishment and publication of open standards for software and systems. The DCGS offers one example. In that case study, DCGS program management responded to a SOCOM need for high-performance reconnected ops DI2E by pressuring the DCGS prime contractor to release the DIB source kernel for open-source collaboration. Using the DIB package, MarkLogic, a supplier of enterprise database software, created an XML database. In the end, the software proved valuable to SOCOM, a specific end-user community with unique, niche requirements.

In addition to revealing systems for open-source innovation, case study analysis also indicates that kit-based and modular approaches to materiel development can contribute to greater integration of end-user needs. The reverse of this is the more traditional platform-based development. Harvest HAWK provides one example of this best practice. In that program, users found the original kit to be

inconvenient because of its weapons release mechanism. Namely, in order to deploy missiles, the system had to first depressurize. The installation of a derringer door into the kit corrected the issue, and was made possible by the fact that the kits are not permanently installed on the C-130J platforms. The roll-on/roll-off nature of the Harvest HAWK capability allows for refinements not requiring significant SoS-level changes. In contrast with this best practice, systems acquired under a traditional model show a heavily diminished ability to integrate changing end-user needs. Future Combat Systems (FCS), for example, folded all capabilities into a slow-moving platform acquisition effort in a way that precluded changes to sub-systems based on new end-user needs.

In either of the two best practices in user needs integration (i.e., open source standards and kit-based development), performance in knowledge ownership and access to knowledge is an important enabler. For this reason, case studies illustrate that open-source publication of standards and basic software is a best practice in the information access attribute. However, revealing the foundation for a system-of-systems alone is not enough to enable stakeholders to develop and refresh sub-systems. This information is only meaningful insofar as leadership in any SoS acquisition effort recognizes that stakeholders across a system-of-systems vary widely in their ability to access, understand, and use information that is available to them.

Systematic and institutional stovepipes are one obstacle to information ownership. Other, less tangible obstacles include lower technical expertise among information consumers, lack of sufficient resources to handle the financial and technical costs of information, and compatibility issues in the recipients' systems with the format or type of information. Therefore, one best practice to facilitate knowledge ownership and access to information is to campaign for—or in the event that the provider of information is also the lead stakeholder for a system-of-systems, to approve and make available—the budgetary and technical resources necessary for information management.

Workforce best practices comprise a third enabling factor in SoS acquisition. Identifying, recruiting, and retaining the most appropriate personnel for any SoS acquisition effort can substantially impact the effort's process and outcomes. However, identifying best practices in this attribute is particularly difficult for two reasons. First, human inputs are unpredictable. In the case of Harvest HAWK, replacing a single engineer rescued the program from a months-long logjam when the new engineer identified an error in a sub-system's code that had been inhibiting the proper function of the system-of-systems. Second, workforce is a complex system in itself; technical and programmatic personnel interact with one another at different levels with unpredictable impacts.

Analysis of the case studies indicates one best practice in the workforce attribute is to balance programmatic and technical personnel based on the specific needs of a program. At the enterprise level, the ideal workforce is weighted toward programmatic workers with some technical personnel available to provide overarching direction. At the systems level, technical personnel are more prevalent in the ideal workforce. Weighting toward technical personnel rather than programmatic personnel allows the workforce to avoid parochial interests and provide metrics-based assessments of progress toward a sub-system's development.

Incorporating recent and one-time end-users into the workforce is an additional best practice that enhances the alignment of outputs with the need they are expected to satisfy. The Deepwater family of vessels has been incorporating this best practice into its efforts to acquire the vessels formerly comprising that system-of-systems. The presence of decision-makers with recent field experience in the Harvest HAWK initiative also contributed to that program's success in producing an effective system-of-systems to meet an urgent operational need on the part of the Marine Corps for close air support.

Regarding the incentive structure of an acquisition effort, analysis indicates fostering and satisfying greater mission commitment among stakeholders is an ideal motivator. Although mission commitment seems intangible and difficult to effect, the case studies highlight different ways to enhance the commitment of personnel throughout an acquisition effort's hierarchy to the effort's values and desired end-state. For example, having strong budgetary advocates at the executive level communicates to stakeholders that their work in the acquisition of a system-of-systems is valuable to the end-user and to the organization as a whole. Analysis indicates that personnel management tools can provide additional incentives. For example, as shown in the Deepwater case, the strategic appointment of accomplished personnel to leadership positions can inspire confidence throughout a program. Similarly, accountability at each level of the personnel hierarchy provides a disincentive to poor performance.

Case study analysis also illustrates that acquisition managers can influence an effort's success through incentives aimed at other systems and organizations. Most notably, high barriers to the entry of new technologies into an acquisition effort act as a disincentive to mid-stream innovation and damage the long-term effectiveness of a system-of-systems. The Harvest HAWK case offers several examples of barriers to entry and their impact on an effort's process and outcomes. At the front end, the Marine Corps did not conduct a competition for source selection on the Harvest HAWK contract. Challenges that emerged later in the development process may have surfaced sooner if competitive offerings had been evaluated. In

contrast with this situation, lower barriers to entry of competitive and more recent technologies in DCGS facilitated the emergence of a competitive database solution that ultimately improved the operability of the entire system-of-systems.

These best practices above represent ways to structure a complex acquisition effort to improve effectiveness and efficiency based on seven of the eight attributes analyzed. Identifying best practices in risk assessment, the final attribute, presents two significant challenges. First, risk is an inherent and unavoidable aspect of complexity. In addition to uncertainties originating in the development and procurement of individual systems, the interactions between and among those systems also creates potential areas of risk. Second, risks emerge in different stages of any given project in ways that cannot be predicted, complicating the universal application of best practices. For example, the Army's approach to FCS exhibited greater risks in the early stages of system development. The effort was particularly risky in its requirements generation processes, which led to the selection of immature and untested technologies. Conversely, Harvest HAWK was non-developmental by default and requirements in the early stages of that acquisition were less risky. It would appear that Harvest HAWK has adopted this as a best practice to reduce and manage risk. In fact, risks were just displaced elsewhere. They emerged when the Marine Corps began piecing existing systems together and creating new interactions for which the sub-systems had not been designed.

Difficulties aside, analysis indicates best practices for the management and assessment of risk exist, but they should be evaluated for their fit with the specific objectives and challenges of an SoS acquisition effort and its unique sub-systems and interactions.

Conclusions

Complexity in defense acquisitions has emerged over time due to several changes in the warfighter's needs. On the demand side, end-users face varied and quickly evolving threats that require constant innovations in materiel and weapons systems. On the supply side, technology development in the private sector and even among user communities often outpaces DoD-led acquisition projects. SoS acquisition is a challenging undertaking, but research and analysis supports this study's premise that SoS approaches performed effectively help the defense community ensure interoperability and obtain technologies at the bleeding edge of the innovation curve.

The trend towards more quickly evolving threats and greater industry- and user-led innovation is not likely to slow. In fact, it is likely to accelerate as the means of innovation become more readily accessible, especially for warfighters innovating their own solutions. As the internal complexity of defense acquisitions grows, and

the interactions of systems-of-systems with other platforms become more numerous and critical, best practices such as those outlined in this report will become increasingly important.

This paper argued that it is particularly critical for the defense acquisition community to incorporate best practices in three governance attributes in particular. Acquirers should find the right balance of enterprise-level organizational focus and program-level technology awareness. In order to accomplish this balance, they must delegate decision-making across their organizations and maintain close managing relationships between oversight entities at the enterprise level, and their technical program components at the capabilities level. Enterprise-level oversight entities must maintain close managing relationships with their capability-level technical entities in order for a complex acquisition effort to succeed within human capital restrictions and with fewer cost and schedule issues.

References

Ackerman, R. (2007, December). Wireless links enhance maritime security. *Signal Online*. Retrieved from http://www.afcea.org/content/?q=node/1431

Army to field Northrop-built counter-mortar system in Iraq. (2005, October 25). *Aerospace Daily*. Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Ben-Ari, G., & Chao, P. (Eds). (2009). *Organizing for a complex world: Developing tomorrow's defense and net-centric systems*. Washington, DC: CSIS.

Berteau, D. J., Ben-Ari, G., & Zlatnik, M. (2009)*. Complex government technology development programs: Meeting the policy challenges.* Paper presented at 2009 Atlanta Conference on Science and Innovation Policy, Atlanta, GA, Georgia Institute of Technology.

Biesecker, C. (2008, July 17). Lieberman suggests DNDO may need budget oversight authority. *Defense Daily*. Retrieved from http://www.defensedaily.com/lieberman-suggests-dndo-may-need-budget-oversight-authority/

Corbett, C., Beigh, B., & Thompson, S. (2012, April–March). Counter-Rocket, Artillery, and Mortar (C-RAM) Joint Intercept Capability: Shaping the future joint force. *Shaping Fires for 2020,* 46–53.

Corrin, A. (2012, May 29). Army to pay $500M for Future Combat Systems termination. *Federal Computer Week*. Retrieved from http://fcw.com/articles/2012/05/29/army-future-combat-systems-500-million-cancellation-fee.aspx

Counter-Rocket, Artillery & Mortar (C-RAM). (2011). *FY 2012 Army Budget Request*. February 2011. Retrieved from http://asafm.army.mil/Documents/OfficeDocuments/Budget/BudgetMaterials/FY12/pforms/opa2.pdf

Defense Information Systems Agency. (2011, October 4). Counter rocket, anti-mortar sense and warn forward operating base (FOB) staffing and operations. Retrieved from FedBizOpps.gov website: https://www.fbo.gov/index?s=opportunity&mode=form&id=22097f2ff3bd069c8c6b84ef3eb44fbb&tab=core&_cview=0

Department of Defense (DoD). (2008, December 8). *Operation of the Defense Acquisition System* (DoD Instruction 5000.02). Washington, DC: Under Secretary of Defense for Acquisition, Training, and Logistics. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf

Department of Defense Information. (2009, September 30). Contracts for September 30, 2009. *FIND*. Retrieved from http://www.defenseprocurementnews.com/2009/09/30/contracts-for-september-30-2009/

Director of Operational Test and Evaluation. (2002, December). Distributed Common Ground/Surface System (DCGS). *FY 2002 Annual Report*. Retrieved from http://www.dote.osd.mil/pub/reports/FY2002/

Director of Operational Test and Evaluation. (2006, December). Counter rocket, artillery and mortar. *FY 2006 Annual Report*. Retrieved from http://www.dote.osd.mil/pub/reports/FY2006/pdf/other/2006DOTEAnnualReport.pdf

DoD finalizes C-130 recap effort for urgent combat needs. (2008, April 23). *Aerospace Daily*. Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Fein, G. (2009, January 27). USCG expands capability to assume deepwater maintenance, logistics. *Defense Daily*. Retrieved from http://www.defensedaily.com/publications/dd/USCG-Expands-Capability-To-Assume-Deepwater-Maintenance-Logistics_5452.html

Four house lawmakers express concern over DCGS-A's abilities, cost. (2013, February 4). *Inside the Army*, *25*(5).

Fuel and fires. (2009, May 25). *Flight International*. Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Gell-Mann, M. (1999). Complex adaptive systems. In G. A. Cowan, D. Pines, & D. Meltzer (Eds.), *Complexity: Metaphors, models, and reality* (pp. 17–29). New York, NY: Westview Press.

Geoff, F. (2009, January 27). USCG expands capability to assume Deepwater maintenance, logistics. *Defense Daily*. Retrieved from http://www.defensedaily.com/publications/dd/USCG-Expands-Capability-To-Assume-Deepwater-Maintenance-Logistics_5452.html

Government Accountability Office (GAO). (2001, May). *Army transformation faces weapon systems challenges* (GAO-01-311). Retrieved from http://www.gao.gov/assets/240/231651.pdf

Government Accountability Office (GAO). (2007a, March). *Assessments of selected weapons programs: Report to congressional committees* (GAO-07-406SP). Retrieved from http://www.gao.gov/assets/260/258416.pdf

Government Accountability Office (GAO). (2007b, March). *Key decisions to be made on future combat system* (GAO-07-376). Retrieved from http://www.gao.gov/assets/260/257754.pdf

Government Accountability Office (GAO). (2011, June). *DOD needs a strategic, risk-based approach to enhance its maritime domain awareness* (GAO-11-621). Retrieved from http://www.gao.gov/new.items/d11621.pdf

Government Accountability Office (GAO). (2012, March*). Assessments of selected weapons programs: Report to congressional committees* (GAO-12-400SP). Retrieved from http://www.gao.gov/assets/590/589695.pdf

Government Accountability Office (GAO). (2013, March). A*ssessments of selected weapons programs: Report to congressional committees* (GAO-13-294SP). Retrieved from http://www.gao.gov/assets/660/653379.pdf

Gorman P., & Diehl R. (2003). *Close support fires for the Army's Objective Force.* Alexandria, VA: Institute for Defense Analyses.

Harvest Hawk tests prove successful. (2012, April 25). *Jane's Defence Weekly.* Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Honeywell has filed a protest. (2004, March 29). *Aviation Week and Space Technology.* Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Hughes, D. (2003, May 19). The Coast Guard. *Aviation Week and Space Technology.* Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Hughes, D. (2004, February 9). Boosting air security. *Aviation Week and Space Technology*. Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Koch, A. (2002, July 3). US Coast Guard begins major modernisation. *Jane's Defence Weekly*. Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Kwak, Y. H., & Smith, B. (2009). Managing risks in mega defense acquisition projects: Performance, policy, and opportunities. *International Journal of Project Management, 27*(8), 812–820. Retrieved from http://home.gwu.edu/~kwak/Managing%20Risks%20in%20Mega%20Defense%20Acuqisition%20Projects.pdf

Levy, D. (2000). Applications of limitations of complexity theory in organization theory and strategy. In J. Rabin, G. J. Miller, & W. B. Hildreth (Eds.), *Handbook of strategic management*. New York, NY: Marcel Dekker.

Lockheed Martin delivers first target sight system to USMC. (2009, July 1). *Aerospace Daily*. Retrieved from LexisNexis® Academic. http://www.lexisnexis.com

Malenic, M. (2009, May 22). Army awaits approval to break FCS into three programs. *Defense Daily.* Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Malenic, M. (2010, January 15). Army chief expects new vehicle program to avoid FCS pitfalls. *Defense Daily*. Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Marines to deploy first KC-130J Harvest Hawk Kit this month. (2010, October 11). *Inside the Navy*. Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Mason, R. (2007). The external environment's effect on management and strategy: A complexity theory approach. *Management Decision, 45*(1), 10–28.

Maxfield, R. (1997, June). Complexity and organization management. In D. Alberts & T. Czerwinski (Eds), *Complexity, global politics, and national security* (pp. 171–218). Washington, DC: National Defense University.

National Defense Authorization Act for Fiscal Year 2006, H.R. 1815, 109 Cong. (2005). Retrieved from http://www.gpo.gov/fdsys/pkg/BILLS-109hr1815enr/pdf/BILLS-109hr1815enr.pdf

Navy looks forward to arrival of DCGS "backbone," official says. (2005, March 22). *Aerospace Daily*. Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Official: KC-130J's Harvest Hawk Kit getting lots of use in theater. (2011, November 7). *Inside the Navy*. Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

O'Rourke, R. (2011, September 9). *Coast Guard Deepwater Acquisition Programs: Background, oversight issues, and options for Congress* (Congressional Research Service Report RL33753). Retrieved from https://www.fas.org/sgp/crs/weapons/RL33753.pdf

O'Rourke, R. (2012, January 20). *Coast Guard Deepwater acquisition programs: Background, oversight issues, and options for Congress* (Congressional Research Service Report 7-5700). Retrieved from http://www.fas.org/sgp/crs/weapons/RL33753.pdf

Pernin, C., Axelband, E., Drezner, J. A., Dille, B. B., Gordon, J., Held, B. J., … Sollinger, J. M. (2002). *Lessons from the Army's Future Combat Systems program* (MG-1206-A). Santa Monica, CA: RAND.

Roosevelt, A. (2012, April 16). MBDA's Viper Strike scores direct hits from Marine Corps aircraft. *Defense Daily*. Retrieved from www.defensedaily.com/mbdas-viper-strike-scores-direct-hits-from-marine-corps-aircraft/

Sapolsky, H. (2009). Models for governing large systems projects. In G. Ben-Ari & P. Chao (Eds.), *Organizing for a complex world: Developing tomorrow's defense and net-centric systems.* Washington, DC: CSIS.

Smith, E. (2006). *Complexity, networking, and effects-based approaches to operations.* Washington, DC: Command and Control Research Program. Retrieved from http://www.dodccrp.org/files/Smith_Complexity.pdf

U.S. Air Force joins Navy in criticizing intel ops and plans. (2009, November 6). *Aerospace Daily.* Retrieved from LexisNexis Academic database. http://www.lexisnexis.com

Jacobs, J. C. (2012, May). U.S. naval aviation and weapons development in review. *Proceedings Magazine*, 138(5).Walker, A. (2010, December 8). *Army Awards PD C-RAM for lifesaving efforts in Iraq*. Retrieved from U.S. Army website: http://www.army.mil/article/49128/

Walker, A. (2011, May 3). *Program director counter-rockets, artillery and mortar transitions to new home*. Retrieved from U.S. Army website: http://www.army.mil/article/55878/

Warwick, G. (1998, April 8). U.S. Coast Guard starts replacement programme. *Flight International*. Retrieved from http://www.flightglobal.com/news/articles/us-coast-guard-starts-replacement-programme-35310/

THIS PAGE INTENTIONALLY LEFT BLANK